The Physics of Quantum Information:

量子情報の物理

―量子暗号, 量子テレポーテーション, 量子計算―

Quantum Cryptography,
Quantum Teleportation,
Quantum Computation

D.Bouwmeester
A.Ekert
A.Zeilinger 編

西野哲朗・井元信之 監訳

小芦雅斗　清水　薫　三原孝志
竹内繁樹　伊藤公平　松本啓史
川畑史郎　森越文明 訳

共立出版

The Physics of Quantum Information:

量子情報の物理

—量子暗号，量子テレポーテーション，量子計算—

Quantum Cryptography, Quantum Teleportation, Quantum Computation

D.Bouwmeester
A.Ekert
A.Zeilinger 編

西野哲朗・井元信之 監訳

小芦雅斗　清水　薫　三原孝志
竹内繁樹　伊藤公平　松本啓史
川畑史郎　森越文明 訳

共立出版

The Physics of Quantum Information

Quantum Cryptography, Quantum Teleportation, Quantum Computation

Dirk Bouwmeester, Artur Ekert, Anton Zeilinger eds.

Translation from the English language edition:
The Physics of Quantum Information edited by
Dirk Bouwmeester, Artur Ekert, Anton Zeilinger.

序　文

情報は物理的方法により保持され，伝送され，処理される．だから情報および計算の概念は物理理論の文脈で記述されるものであり，情報についての研究は最終的には実験化が要求される．この一見何でもないように見える言明は自明でない結果を導く．

ムーアの法則によれば，18ヶ月ごとにマイクロプロセッサの処理速度は倍になるが，そのスピードアップを実現する唯一の方法は小さくすることと思われる．そう遠くない将来，論理ゲートは数えるほどの原子しか含まないほどに小さくなるであろう．そうなれば量子力学的効果が重要となる．したがって，コンピュータが速くなり続ける（したがって小さくなり続ける）ならば，新しい量子テクノロジーが現行のものに取って代わるかあるいは補完せざるを得ない．ところが，そのようなテクノロジーは，単にマイクロプロセッサを小さくしたり速くしたりするだけではないことがわかってきた．近年の理論的研究により，量子力学は通信や計算における新しい方法を提供するのに適した性質を備えていること，およびそれは古典的な方法に比べて遙かに強力であることがわかってきた．

この新しい量子テクノロジーはあちこちの研究室で実現されつつある．種々の量子力学的単一粒子がこれまでにないほどの高精度で制御されたり操作されるような実験がこの20年間で実現されてきた．量子力学の黎明期において有名だったいろいろな「思考実験」が実行されるようになった．新しい実験技術により個々の量子系で符号化された情報を保持したり処理したりするこ

とが可能となった．その結果，新しく羽ばたく分野——量子情報処理——が生まれ，それはコンピュータ科学や情報科学と結びついて，量子力学の原理をはるかに豊穣なものにしている．この分野の広がりは物理法則における新しい原理の側面からコンピューティングや通信業における実用化の可能性まで非常に広い範囲に及ぶ．

この分野を振興させる努力は世界的になされているが，その一つとして，ヨーロッパ委員会はTMR（Training and Mobility of Researchers: 研究者の研鑽と流動性向上）プログラムの一環としてネットワーク「量子情報の物理」を支援している．本書の各章は主にこのネットワークにさまざまな形で協力しているメンバーによって書かれた．そして本書がこの基本的かつ新しい分野の教科書的入門書となることを目指している．また多くの章においてTMR以外の研究者たちによる重要な成果も紹介している．しかし，この分野の完全な専門的レビューを行うことがわれわれの目的ではない．この研究分野は極めて活発になってきているので，どんなに包括的なレビューも早晩陳腐なものになってしまうだろう．本書では量子エンタングルメント，量子暗号，量子テレポーテーション，量子計算，量子アルゴリズム，量子状態のデコヒーレンス，量子誤り訂正，量子通信における理論および実験的トピックスについて扱う．

量子力学についてそこそこの知識をもち量子情報がもたらす可能性についての純粋な興味を——われわれもそうであるが——もっているすべての人たちに本書が貢献できるならば幸いである．

最後に，本書における多くの図の作成に関してトーマス・ジェネウェイン(Thomas Jennewein) に謝意を表したい．

2000 年 3 月

オクスフォード，ウィーン

ダーク・バウミースター (Dirk Bouwmeester)
アルトゥール・エカート (Artur Ekert)
アントン・ツァイリンガー (Anton Zeilinger)

目　　次

執筆者一覧

H. Baldauf
Sect. 5.3
Max–Planck–Institut
für Quantenoptik
Hans–Kopfermann–Str. 1
85748 Garching, Germany

R. Blatt
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

S. Bose
Sect. 3.11
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

D. Bouwmeester
Chap. 1, Sects. 3.1–3.3, 3.5–3.10, 6.3
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

H.-J. Briegel
Sects. 6.2, 8.2, 8.6, 8.7
Sektion Physik
Ludwig–Maximilians–Universität
Theresienstrasse 37
80333 München, Germany

M. Brune
Sect. 5.2
Laboratoire Kastler Brossel
Département de Physique
de l'Ecole Normale Supérieure
24 rue Lhomond
75231 Paris, Cedex 05, France

J.I. Cirac
Sects. 4.3, 6.2, 8.6, 8.7
Institut für Theoretische Physik

Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

M. Daniell
Sect. 6.3
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

D. Deutsch
Sect. 4.1
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

W. Dür
Sects. 8.6, 8.7
Institut für Theoretische Physik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

A. Ekert
Chap. 2, Sects. 4.1, 7.2, 7.6
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

S.J. van Enk
Sects. 6.2, 8.6
Norman Bridge Laboratory of Physics
California Institute
of Technology 12-22
Pasadena, California 91125, USA

J. Eschner
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

N. Gisin
Chap. 2, Sects. 3.4, 8.3
University of Geneva
Group of Applied Physics
20 Rue de l'Ecole de Médecine
1211 Geneva 4, Switzerland

S. Haroche
Sect. 5.2
Laboratoire Kastler Brossel
Département de Physique
de l'Ecole Normale Supérieure
24 rue Lhomond
75231 Paris, Cedex 05, France

S.F. Huelga
Sect. 7.6
Departamento de Fisica
Universidad de Oviedo
Calvo Sotelo s/n.
33007 Oviedo, Spain

B. Huttner
Chap. 2, Sect. 8.3
University of Geneva
Group of Applied Physics

20 Rue de l'Ecole de Médecine
1211 Geneva 4, Switzerland

H. Inamori
Chap. 2
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

J.A. Jones
Sect. 5.4
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

R. Jozsa
Sect. 4.2
Department of Computer Science
University of Bristol
Merchant Venturers Building
Woodland Road
BS8 1UB Bristol, England

P.L. Knight
Sects. 3.11, 6.4, 7.3, 8.5
Optics Section
Blackett Laboratory
Imperial College London
London SW7 2BZ, England

W. Lange
Sect. 5.3
Max–Planck–Institut
für Quantenoptik
Hans–Kopfermann–Str. 1
85748 Garching, Germany

D. Leibfried
Sect. 5.2
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

C. Macchiavello
Sects. 7.4, 7.6, 8.4
Dipartimento di Fisica "A.Volta"
and INFM-Unité di Pavia
via Bassi 6
27100 Pavia, Italy

M. Murao
Sect. 8.5
Optics Section
Blackett Laboratory
Imperial College London
London SW7 2BZ, England

H.C. Nägerl
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

G.M. Palma
Sects. 7.2, 7.4
Dipartimento di Scienze Fisiche
ed Astronomiche & unita'INFM
via Archirafi 36

90123 Palermo, Italy

J.-W. Pan
Sects. 3.7, 3.10, 6.3
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

M.B. Plenio
Sects. 6.4, 7.3, 7.6, 8.5
Optics Section
Blackett Laboratory
Imperial College London
London SW7 2BZ, England

S. Popescu
Sect. 8.5
5BRIMS Hewlett–Packard
Laboratories
Stoke Gifford
Bristol BS12 6QZ, England

J.F. Poyatos
Sect. 4.3
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

J.-M. Raimond
Sect. 5.2
Laboratoire Kastler Brossel
Département de Physique
de l'Ecole Normale Supérieure
24 rue Lhomond
75231 Paris, Cedex 05, France

J.G. Rarity
Sect. 3.4
DERA Malvern
St. Andrews Road, Malvern
Worcester WR14 3PS, England
and
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

F. Schmidt-Kaler
Sects. 5.2, 5.3
Institut für Experimentalphysik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

A. Steane
Sect. 7.5
Centre for Quantum Computation
Clarendon Laboratory
University of Oxford
OX1 3PU Oxford, England

K.-A. Suominen
Sect. 7.2
Helsinki Institute of Physics
PL 9, FIN-00014 Helsingin
Yliopisto, Finland

V. Vedral
Sects. 3.11, 6.4, 8.5
Centre for Quantum Computation
Clarendon Laboratory

University of Oxford
OX1 3PU Oxford, England

G. Weihs
Sect. 3.4
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

H. Weinfurter
Chap. 2, Sects. 3.1–3.3, 3.5–3.7, 3.10, 6.3
Sektion Physik
Ludwig–Maximilians–Universität München
Schellingstr. 4/III
80799 München, Germany

H. Walther
Sect. 5.3
Max–Planck–Institut für Quantenoptik
Hans–Kopfermann–Str. 1
85748 Garching, Germany

A. Zeilinger
Chap. 1, Sects. 3.1–3.3, 3.5–3.7, 3.10, 6.3
Institut für Experimentalphysik
Universität Wien
Boltzmanngasse 5
1090 Wien, Austria

P. Zoller
Sects. 4.3, 6.2, 8.6, 8.7
Institut für Theoretische Physik
Universität Innsbruck
Technikerstrasse 25
6020 Innsbruck, Austria

訳者一覧

井元信之（いもと のぶゆき）：第 1 章担当

小芦雅斗（こあし まさと）：第 2 章担当
略歴：1995年　東京大学理学系研究科博士課程修了
　　同　年　日本学術振興会特別研究員
　　同　年　NTT 基礎研究所
　　1999年　総合研究大学院大学先導科学研究科助教授
　　2004年　大阪大学大学院基礎工学研究科助教授
現在：大阪大学大学院基礎工学研究科准教授，博士（理学）

清水 薫（しみず かおる）：第 3 章担当
略歴：1990年　早稲田大学大学院理工学研究科博士前期過程修了
　　同　年　日本電信電話株式会社入社
現在：日本電信電話株式会社 NTT 物性科学基礎研究所主幹研究員

三原孝志（みはら たかし）：第 4 章担当
略歴：1997年　北陸先端科学技術大学院大学情報科学研究科博士後期課程修了
　　同　年　九州東海大学工学部講師
　　2000年　同大応用情報学部助教授
　　2007年　退職
現在：博士（情報科学）

西野哲朗（にしの てつろう）：第 4 章担当

竹内繁樹（たけうち しげき）：第 5 章担当
略歴：1993年　京都大学理学研究科修士課程修了
　　同　年　三菱電機中央研究所
　　1999年　北海道大学電子科学研究所講師
　　2000年　同助教授
現在：北海道大学電子科学研究所・准教授，博士（理学）

伊藤公平（いとう こうへい）：第 5 章担当
略歴：1994年　カリフォルニア大学バークレー校，Ph. D.
　　1995年　慶應義塾大学理工学部助手
　　1998年　慶應義塾大学理工学部専任講師
　　2002年　慶應義塾大学理工学部助教授
現在：慶應義塾大学理工学部教授，Ph.D.

松本啓史（まつもと けいじ）：第 6 章担当
略歴：1995年　東京大学大学院工学系研究科修士課程修了
　　同　年　東京大学工学部計数工学科助手
　　2000年　科学技術振興事業団今井量子計算機構プロジェクト技術参事
　　2003年　国立情報学研究所助教授
現在：国立情報学研究所情報学プリンシプル研究系准教授，博士（数理科学）

川畑史郎（かわばた しろう）：第 7 章担当
略歴：1998年 大阪市立大学工学研究科博士課程修了
同　年 通産省電子技術総合研究所電子基礎部
2001年 産業技術総合研究所 ナノテクノロジー研究部門
2005年 NTT 物性科学基礎研究所客員研究員
2006年 オランダ Twente 大学 在外研究員
現在：産業技術総合研究所ナノテクノロジー研究部門主任研究員，工学博士

森越文明（もりこし ふみあき）：第 8 章担当
略歴：2000年 北海道大学大学院理学研究科博士後期課程修了
2000年 NTT 物性科学基礎研究所 リサーチアソシエイト
現在：NTT 物性科学基礎研究所 研究主任，科学技術振興機構さきがけ「量子と情報」研究員兼務（2004年～2008年），博士（理学）

第1章

量子情報の物理：基本概念

1.1　重ね合わせの原理

重ね合わせの原理は量子情報に関するあらゆる考察の中で，また量子力学のほとんどの思考実験において，そしてパラドクスに関しても，最も中心的な役割を演ずる．それを理論的にあるいは抽象的に述べる代わりに，ここではその精髄を抽出する実験つまり2重スリットの実験で説明しよう（図1.1）．Feynmanによれば，2重スリットにこそは「量子力学の神髄が含まれている」[1]．実験材料は基本的に粒子源，2重スリット，干渉縞を観察するためのスクリーンである．この干渉縞は，粒子源から出射される粒子がもつ波としての性質として理解される．この実験はいろいろな粒子に対して行われていることを言っておこう．すなわち光子[2]，電子[3]，中性子[4]，そして原子[5]でも行われている．これらの実験における粒子の量子状態は

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_a\rangle + |\Psi_b\rangle\right) \qquad (1.1)$$

というコヒーレントな重ね合わせの状態である．ただし，$|\Psi_a\rangle$ および $|\Psi_b\rangle$ はそれぞれスリット a および b のみが開いているときの状態である．

ここでおもしろいのは，これまでの実験でも確認されていることであるが，この干渉縞は粒子一つひとつを数え上げることによっても——すなわち粒子一つだけがそれ自身と干渉するような微弱な強度においても——観測されるという点である．このような場合，粒子が実際どちらのスリットを通ったの

かと聞きたくなるであろう．標準的な量子力学によると,「粒子はどちらのスリットを通ったのか？」という質問に対してはそれを確認する実験をしない限り意味のある言明はできない，というのが答えになる．そこで今度はどちらを通ったかを確認する実験をすると，それがどんなものであっても，粒子と相互作用しないわけにはいかず，干渉性の喪失すなわちデコヒーレンスをもたらす．どちらのスリットを通ったか原理的にもわからないような場合にのみ干渉縞が観測されるのである．ここで，しばしばそう思われることもあるが，粒子が二つのスリットを同時に通ったという言明も成り立たないことも注意しておこう．これは局所的なものという粒子の定義そのものに矛盾しているし，またこの言明には実際上の意味は何もない．最後に，干渉性をある程度失うことを代償とするなら，どちらのスリットを通ったかについての知識をある程度得ることができることも指摘しておこう．

1.2　量子ビット

情報科学において最も基本となるのはビットである．これは “0” と “1” のどちらかの値を取り得る一つの系である．機械的なスイッチを思い浮かべればわかるように，ビットは古典的な実現として二つの識別可能な状態をもち，その二つの状態は勝手に切り替わること——これは明らかに望ましくないことであるが——はないように設計される．

ビットの量子力学版である量子ビット (qubit)[6] も 2 状態の系であり，二つの状態は $|0\rangle$ および $|1\rangle$ と書かれる（訳注：読み方は 0 ケットおよび 1 ケット）．基本的に二つの状態をもつどんな系も量子ビットになり得る．実際，まさにいろいろな可能性が考えられ，多くのものが実験的に実現されている．量子状態にビットを符号化するときの基本的性質はコヒーレンス（可干渉性）と重ね合わせである．すなわち一般的な状態は

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.2}$$

と書かれる．ただし $|\alpha|^2 + |\beta|^2 = 1$ である．この式の意味するところは量子ビットの値は 0 と 1 の間のどこかであるということではない．その意味するところは 0 と 1 の重ね合わせの状態であり，その量子ビットを観測したとき

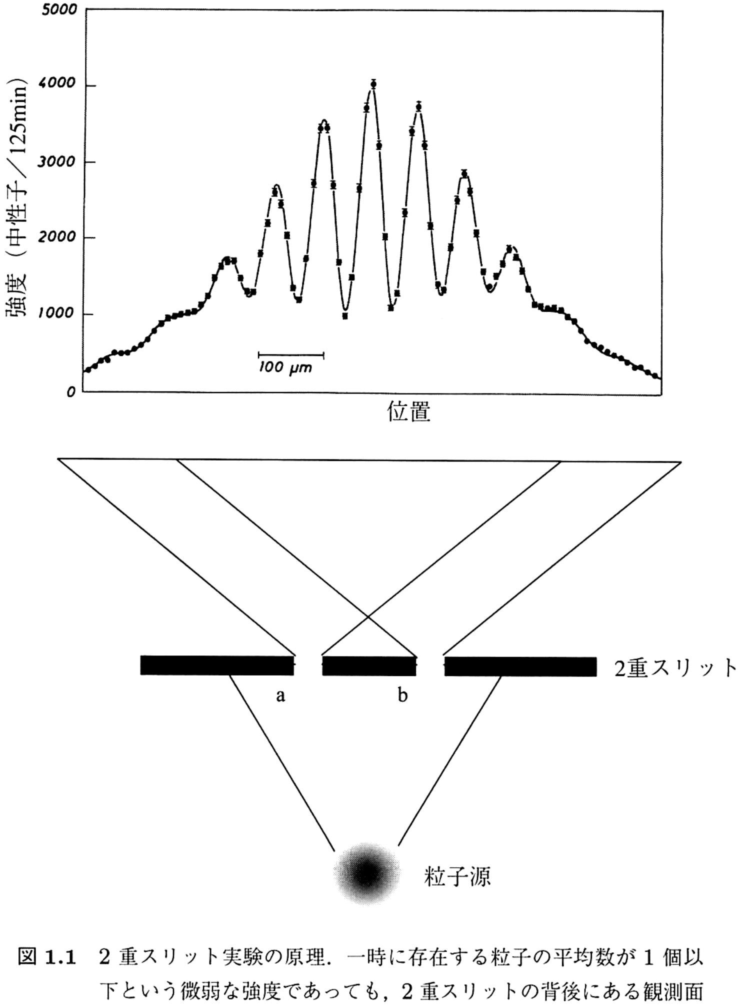


図 1.1　2 重スリット実験の原理．一時に存在する粒子の平均数が 1 個以下という微弱な強度であっても，2 重スリットの背後にある観測面に干渉縞が現れる．ここに示したのは中性子干渉によって得られた実験データ [4] である

"0" を得る確率が $|\alpha|^2$ で "1" を得る確率が $|\beta|^2$ ということである．すなわち

$$p(\text{“0”}) = |\alpha|^2\,, \quad p(\text{“1”}) = |\beta|^2 \tag{1.3}$$

である．この量子ビットの定義によれば，ビットのもっていた「確定性」を失うように思われるかもしれない．しかし重要なことは，式 (1.2) は "0" と "1" のインコヒーレントな（すなわち確率的な，あるいはランダムな）混合なのではなく，コヒーレントな（すなわち，$|0\rangle$ と $|1\rangle$ が位相関係を保った）重ね合わせであるという点である．核心は，コヒーレントな重ね合わせにおいてはその量子ビットの値を確定させるような基底がいつでも選べるのに対し，インコヒーレントな混合においてはどんな基底を選ぼうと常に混合状態である点にある．たとえば

$$|Q'\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{1.4}$$

のような例を考えてみよう．この状態は明らかに "0" または "1" に見いだされる確率は 50 %であることを意味する．ところがおもしろいことに，ヒルベルト空間で 45 度回転した基底においてはこの状態は確定状態となる．これは量子ビットに簡単な変換を施せばわかる．量子情報理論において最も基本的な変換はアダマール変換であるが，その作用は

$$H|0\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\,, \quad H|1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{1.5}$$

で表される．これを $|Q'\rangle$ に作用させると

$$H|Q'\rangle = |0\rangle \tag{1.6}$$

となって，確定した状態となる．混合状態ではこうなることはない．

1.3　単一量子ビットの変換

量子情報物理の最も基本的な実験には，簡単な 50/50 ビームスプリッタ（透過率・反射率とも 50%）により考察できるものが少なからずある．このようなビームスプリッタは光子のみならず種々の粒子に対して実現できている．図 1.2 に示すように，一般的ビームスプリッタにおいて二つの入力と二つの出力がある場合を考えよう．

50/50 ビームスプリッタ上方あるいは下方から入射した粒子が上方または下方に出射する確率はいずれも 50%である．この場合，量子力学的なユニタリ発展の条件――すなわち，粒子が吸収されることがないという条件――によりビームスプリッタの作用にある位相シフトの関係が課される [7]．このとき任意に選んでよい位相の自由度が一つ残るが，最も簡単なのは式 (1.5) のアダマール変換に一致するように選ぶことである．

入射する粒子の状態は一般的な量子ビット状態

$$|Q\rangle_{\mathrm{in}} = \alpha|0\rangle_{\mathrm{in}} + \beta|1\rangle_{\mathrm{in}} \tag{1.7}$$

であるとしよう．これは粒子を上方入力に見いだす確率振幅が α で下方に見いだす確率振幅が β であることを意味する．これにビームスプリッタが作用すると，出力状態は

$$|Q\rangle_{\mathrm{out}} = H|Q\rangle_{\mathrm{in}} = \frac{1}{\sqrt{2}}\left((\alpha+\beta)|0\rangle_{\mathrm{out}} + (\alpha-\beta)|1\rangle_{\mathrm{out}}\right) \tag{1.8}$$

となる．粒子を上方出力に見いだす確率振幅は $\alpha+\beta$ で，下方に見いだす確率振幅は $\alpha-\beta$ となる．$\alpha=0$ または $\beta=0$ の特別な場合，粒子を上方出力または下方出力に見いだす確率は等しくなる．

このようなビームスプリッタの直列接続は連続するアダマール変換の列を実現する．二つが続く場合はマッハ-ツェンダー干渉計となる（図 1.3）．

図において 2 枚のミラーはビームの方向を変えるだけで量子状態には何も作用しないので，理論的には無視してよい．すると干渉計全体の作用はアダマール変換を 2 回行うことになり，式 (1.7) で表される任意の入力状態に対し

$$|Q\rangle_{\mathrm{out}} = HH|Q\rangle_{\mathrm{in}} = 1Q\rangle_{\mathrm{in}} \tag{1.9}$$

となる．これは式 (1.5) のアダマール変換を 2 回施すと恒等変換になることから明らかである．これは図 1.3 に示したような出力ミラーを含むマッハ-ツェンダー干渉計は入力をそのまま出すことを意味する．再び極端なケースすなわち一つのビームだけに粒子がある場合を想定しよう．たとえば，下方の入力には何も入れず $\alpha=1$ とする．すると式 (1.9) によれば粒子は確実に上方に見いだされる．ここでおもしろいことは，この結果は二つのビームスプリッタの間にある二つの道筋で粒子が等確率で（ただし一定の位相差で）見いだ

されることの帰結である点である．確実に上方に見いだされ下方に絶対現れないという結果は，2 枚めのビームスプリッタに入射する二つの振幅の干渉によるものである．

量子情報の言い方をすれば，量子ビットの初期状態が確定的であるならば，他に細工のないマッハ－ツェンダー干渉計を通過後の状態も確定的である．そしてこれは，二つのアダマール変換の間で量子ビットの状態が最大限不確定となっていることの帰結である，ということになる．

アダマール変換以外の重要な量子ゲートは位相シフタである．図 1.4 に位相シフタを挿入したマッハ－ツェンダー干渉計を示す．位相シフタの役割は単に確率振幅の位相を φ だけ回すことである．特に二つのビームの片方のみ位相シフトすることに意味があり，図のようにここでは例えばそれを上方のビームとする．このような位相シフタの作用は，われわれの記法で

$$\Phi|0\rangle = e^{i\varphi}|0\rangle\,, \quad \Phi|1\rangle = |1\rangle \tag{1.10}$$

のようなユニタリ変換で表される．したがって，全体の出力は関係するすべての変換を次々と入力に施すことにより

$$|Q\rangle_{\text{out}} = H\Phi H|Q\rangle_{\text{in}} \tag{1.11}$$

と表される．一般の入力状態に対する出力状態の表式を求めるのは読者に任せ，ここでは再び $\alpha = 1$ かつ $\beta = 0$ すなわち $|Q\rangle_{\text{in}} = |0\rangle$ の場合に限定しよう．すると最終的に

$$H\Phi H|0\rangle = \frac{1}{2}\left((e^{i\varphi}+1)|0\rangle + (e^{i\varphi}-1)|1\rangle\right) \tag{1.12}$$

が得られる．この解釈は簡単である．まず $\varphi = 0$ に対しては量子ビットの値は確実に "0" である．一方，$\varphi = \pi$ に対しては "1" である．つまり，φ の位相シフトにより量子ビットの出力を 0 と 1 の間で切り換えることができる．一般の φ では量子ビットが値 "0" を取る確率は $P_0 = \cos^2(\varphi/2)$ で，"1" を取る確率は $P_1 = \sin^2(\varphi/2)$ である．

この節では量子ビットに対する線形変換について基本的な記述について説明した．次にエンタングルした量子ビットの話に移る．

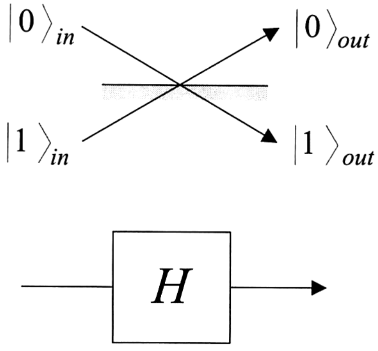


図 1.2　50/50 ビームスプリッタ（上図）と対応するアダマール変換 H のダイアグラム（下図）

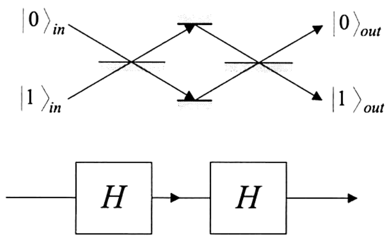


図 1.3　マッハ－ツェンダー干渉計（上図）は連続する 2 回のアダマール変換である（下図）

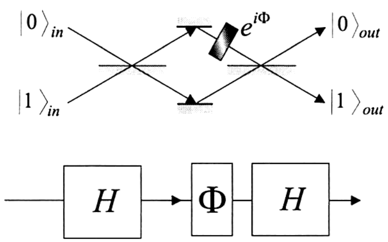


図 1.4　上図：片方の経路に位相シフト φ を含むマッハ－ツェンダー干渉計．下図：対応するダイアグラム．2 回のアダマール変換と位相シフトゲートを含む

1.4　エンタングルメント

一つの粒子を左方に，他方の粒子を右方に同時にペアで放出するような粒子源を考えよう（図 1.5）．これらの粒子は反対の運動量（訳注：方向まで含めて）をもつとしよう．すると左方の粒子（粒子 1）が上方ビームに見いだされれば右方の粒子（粒子 2）は必ず下方ビームに見いだされる．同様に粒子 1 が下方ビームに見いだされれば粒子 2 は必ず上方ビームに見いだされる．量子ビットの言葉で言えば，二つの量子ビットは逆の値を運ぶ．粒子 1 が値 “0” を運ぶならば粒子 2 は値 “1” を運び，逆ならその逆である．量子力学的に言えば，これは

$$\frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 + e^{i\chi}|1\rangle_1|0\rangle_2\right) \tag{1.13}$$

という 2 粒子の重ね合わせ状態である．位相 χ は粒子源の内部的性質によるもので，簡単のため $\chi = 0$ とおく．式 (1.13) はエンタングル状態[1]と呼ばれる [8]．おもしろいのはいずれの量子ビットも確定的値をもたないのに，一つの量子ビットの値を測定した途端（その値はランダムであるが），もう一方の量子ビットの値が逆になっている．その測定はいくらでも離れた場所で行われても構わないので，つまりこれが量子力学的非局所性 (non-locality) の謎なのである．

最もおもしろいことが起こるのは，この二つの量子ビットが図 1.5 のように位相シフトとアダマール変換を受けるときである．このとき，それぞれのアダマール変換の後での粒子検出に対して，すなわちビームスプリッタの後での 2 粒子干渉 [10] を確認しようとするとき，ベルの不等式と呼ばれる局所性を破る非局所的相関が観測されるのである．ここで理論的な詳細に立ち入ることは避けるが（詳しくは 1.7 節参照），そのような不等式の破れはそれぞれの量子ビットの局所的な性質に基づく相関では説明はできない．この場合の両サイド間の量子的相関は，片方のディテクタが実験パラメータのセッティング——つまりもう片方の粒子の位相の選択——に影響を受けていないと仮定すると説明できない．ベルの不等式の意味を正確に解説する方法はいくらもあり，形式的な記述方法もいくらもある．そのおよそは 1.7 節で述べるが，あとは文献を挙げておく（たとえば文献 [12] とその引用文献）．

---

[1] Entanglement は Schrödinger[9] が 1935 年に導入した *Verschränkung*（訳注：腕組みとか交差を意味するドイツ語）の意訳．

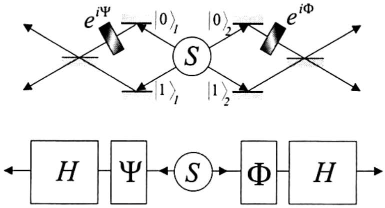


図 1.5　エンタングルした 2 粒子を発生する粒子源．上図：2 粒子干渉計によるエンタングルメントの検証．下図：1 光子ゲートによるダイアグラム

二つ以上の量子ビットへの一般化は非常におもしろく，かつ量子計算に密接な関係が出てくる．簡単な例として，図 1.6 のような三つの量子ビットを考えてみよう．ここで粒子源は GHZ 状態（Greenberger-Horne-Zeilinger 状態）と呼ばれる

$$\frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3) \tag{1.14}$$

という状態（[13] および 6.3 節）を発生すると仮定しよう．この状態は大変特異な性質をもつ．まず 2 粒子エンタングルメントのときと同じく，単独の量子ビットではビット値は確定しておらず何の情報ももたない．しかしどれかの量子ビットの値が測定されると残りの二つも，0-1 基底で測定される限り確定してしまう．この性質はそれぞれの測定がどんなに離れていようと無関係に成り立つ．

最もおもしろいことは，3 か所での測定が位相シフタとアダマール変換のあとで行われたとしても，特定のセッティングのもとでは完全な相関があることに変わりがないことが，式 (1.14) から予測されることである．このことは単に統計的な予測だけでなく，確定的な予測においても量子力学が局所実在論に基づく古典論とは異なることを意味する．

1.5　エンタングルメントと識別不可能性

エンタングルメントの性質と発生法を理解するためには，式 (1.13) や式 (1.14) が直積状態の重ね合わせになっていることに着目しなければならない．1.1 節の 2 重スリットの回折現象の議論から，重ね合わせとはその和になって

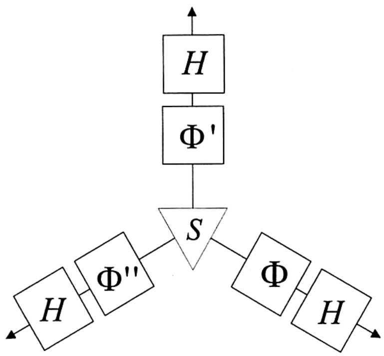


図 **1.6**　GHZ 状態にある3粒子エンタングルメント．ここでは基本ゲートによる表現のみを示す．3粒子干渉計による物理的実現法は読者にとって明白であろう

いる二つの可能性のどちらが起こっているのかを，知る手立てがないものであることを思い出そう．この規則がエンタングルメントの理解のためにもそのまま適用される．たとえば

$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2) \tag{1.15}$$

という状態において，量子ビット1も量子ビット2もそれが値0であるか1であるかは確定していない．しかし観測により一方の値が測定されると即座にもう片方の値が決まってしまう．このような性質がエンタングルメントをどのように発生し観測するかに直接結びつく．

エンタングルメントを発生するためには，可能性が複数なければならない．まず物理的構成を工夫することにより，先に述べた識別不可能性を初めから内在するような粒子源を作ることができる．たとえば，スピン0の粒子がスピン1/2の二つの粒子に分裂するような内部角運動量保存緩和現象において実現される [15]．この場合，それぞれの粒子のスピンの値は逆でなければならない．その値を粒子原の段階で判定する方法がないとすれば，発生される量子状態は

$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2) \tag{1.16}$$

である．ただし $|\uparrow\rangle_1$ などは粒子1が上向きスピンをもつ状態を意味する．式 (1.16) の状態は回転に対して不変である——すなわちどの方向であろうとも

スピンが反平行である——という著しい性質をもつ．

2番めの可能な発生法として，式 (1.15) のような重ね合わせの成分であるそれぞれの状態を，粒子が識別できるようなやり方で実際に発生する粒子原を使う方法が考えられる．たとえば，タイプIIのパラメトリック下方変換 [16]（3.4.4項）では，特定の方向に対して

$$|H\rangle_1|V\rangle_2 \quad \text{および} \quad |V\rangle_1|H\rangle_2 \tag{1.17}$$

という2光子状態を発生する．これは，光子1が水平偏光で光子2が垂直偏光，あるいは光子1が垂直偏光で光子2が水平偏光のどちらかのケースである状態である．しかし，パラメトリック光学結晶中での H 偏光と V 偏光の速度が異なるため，二つのケースの間で二つの光子の時間関係が異なる．したがって，式 (1.17) の二つの項は時間計測によって区別することができ，そのためにエンタングルした状態は発生しない．ところがこの場合でも，二つの光子のずれたタイミングを戻して区別できないようにすると，エンタングルメントを発生することができる．これは量子消しゴムの手法 [17] の応用であり，二つの光子の時間順序を示すマーカーを消すことに相当する．これにより最終的な量子状態は

$$|\Psi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 + e^{i\chi}|V\rangle_1|H\rangle_2\right) \tag{1.18}$$

というエンタングル状態になる．

3番めの方法はエンタングルしていない状態を強制的にエンタングルした状態に射影することによって得られる．エンタングルした状態はその重ね合わせのどの成分とも直交していないことに注意しよう．今，エンタングルしていない

$$|0\rangle_1|1\rangle_2 \tag{1.19}$$

という状態が射影演算子

$$P = |\Psi\rangle_{12}\langle\Psi|_{12} \tag{1.20}$$

で記述されるフィルタに送られたとしよう．$|\Psi\rangle$ は式 (1.15) の状態である．すると当然

$$\frac{1}{2}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right)\left(\langle 0|_1\langle 1|_2 + \langle 1|_1\langle 0|_2\right)|0\rangle_1|1\rangle_2 = \frac{1}{2}\left(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\right) \tag{1.21}$$

となる．ちなみに，射影は量子ビットの逸失を伴うので上式は規格化されていない．

上に議論した三つの方法はエンタングルした状態を出力する方法として原理的に使えるが，さらに状態の測定に基づくエンタングルメントの発生方法もある．すなわち，一般にエンタングルしていない状態あるいは部分的にしかエンタングルしていない状態があるとして，それを上記のフィルタと同様にエンタングルした状態に射影するような測定である．これは三つの光子による GHZ エンタングルメントの最初の実験に使われた（6.3 節参照）[18].

1.6　制御 NOT ゲート

これまで 1 量子ビットゲートすなわち単一の量子ビットだけを対象としたゲートを考えてきた．しかし，量子計算の応用において最も重要なのは 2 量子ビットゲートである．これは一つの量子ビットの状態の変化が他方の量子ビット状態に依存するようなものである．その最も簡単なゲートである「制御 NOT」(controlled NOT) を図 1.7 に示す．制御 NOT のエッセンスは，制御量子ビットが論理値 1 をとるときおよびそのときに限り標的量子ビットが反転することにある．制御量子ビットそのものは値を変えない．制御 NOT の作用は

$$\begin{aligned} |0\rangle_c|0\rangle_t &\to |0\rangle_c|0\rangle_t \qquad |0\rangle_c|1\rangle_t \to |0\rangle_c|1\rangle_t \\ |1\rangle_c|0\rangle_t &\to |1\rangle_c|1\rangle_t \qquad |1\rangle_c|1\rangle_t \to |1\rangle_c|0\rangle_t \end{aligned} \tag{1.22}$$

によって表される．ただし $|0\rangle_c$ と $|1\rangle_c$ は制御量子ビットの状態で，$|0\rangle_t$ と $|1\rangle_t$ は標的量子ビットの状態である．制御 NOT は 1.3 節の 1 量子ビットゲートと併せ，量子計算のネットワークを実現するのに用いられる．特におもしろい応用として，これらの量子論理ゲートを用いて 2 量子ビットや多量子ビットのエンタングル状態を発生することができる．

1.7　EPR パラドクスとベルの不等式

Einstein と Bohr の論争 [20] に顕著に見られるように，量子力学が新奇で直観に反する性質をもつことは量子力学が発見された直後から議論されてきた．当初 Einstein は量子力学に自己矛盾があることを示そうとしたが，後に量子

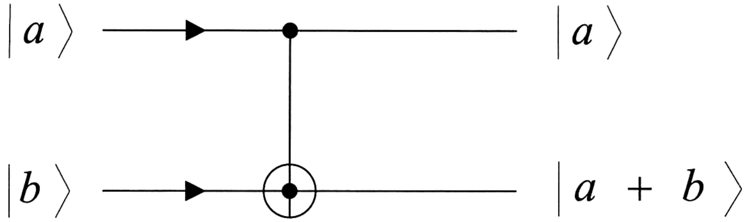


図 1.7 制御 NOT は二つの量子ビットに関する変換である．制御量子ビット（上方）の値に依存して下方の量子ビット値が変化する．下方の量子ビットの値は上の量子ビットが値 1 をとるとき反転し，値 0 をとるとき反転しない．これは「足して 2 で割り余りを求める」ことと同じである

力学が不完全であることを示そうとする議論に組み立てていった．Einstein, Podolsky，Rosen (EPR) はその独創的な論文 [21] において，二つの粒子のそれぞれの位置と運動量は確定していないが，重心（位置の加重平均値）と運動量差は確定しているような 2 粒子系を考察した．これは，片方の粒子の位置または運動量を測定するともう一方の粒子に作用することなくその位置または運動量が確定することを意味する．二つの粒子が十分離れた場合，EPR は粒子 1 に対する測定は粒子 2 に何の影響も与えない（局所性の条件）と仮定した．すなわち，粒子 2 の性質は粒子 1 の測定とは独立であるはずである．これより粒子の位置と運動量は同時に確定できることになってしまう．

これに対し Niels Bohr は，その有名な回答 [22] において次のように述べた．すなわち，EPR の 2 粒子はそれぞれ常に全体系の一部であるので，片方の粒子に対する測定は全系に関する予測を —— したがってもう一方の粒子についても —— 変えるのである．

この EPR-Bohr の論争は長いこと単なる哲学的なものと見なされてきたが，1951 年に David Bohm[15] はエンタングルしたスピン系を提案し，1964 年に John Bell[23] はそのようなエンタングルした系においては，測定結果を得る以前から —— つまり測定結果とは独立に —— 系の性質が決まっていたと仮定したのでは説明できない相関が量子力学的に導かれることを示した．この量子力学の予想する相関を支持する実験がいろいろなされてきた [24]-[26] が，論理的厳密性の観点からすると，これらの実験にはまだ局所実在論を用いて少

なくとも原理的に説明できてしまうような抜け穴が完全には塞がれていない [27].

ここでベルの原論文の不等式と同等な不等式を導く議論を紹介しよう．図 1.8 のように，二つの量子ビットを放出する粒子源を考える．二つの粒子はエンタングルしており，その状態は

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2\right) \tag{1.23}$$

とする．片方の量子ビットはアリス（図 1.8 では左方）へ，もう一方はボブ（右方）へ送られる．アリスとボブは偏光ビームスプリッタとその二つの出力ポートに置かれた単一光子検出器を用いて偏光測定を行う．アリスは検出器 1 または 2 によるそれぞれ等確率の検出に対応して，測定結果 “0” または”1” を得る．これはアリスがどの偏光基底を選ぶかに関係なく，測定結果は完全にランダムとなる．しかしボブが同じ偏光基底を選んだ場合，ボブも同じ測定結果を得る．したがって EPR の論理展開の最初のステップによれば，アリスはボブが何を得るか確実に予測できることになる．第 2 のステップは局所性の仮説で，アリスの装置からボブの装置への影響は瞬時には伝わらない，すなわちボブの測定結果はボブの得た量子ビットと彼の測定装置にのみ依存するとする．ベルはこの二つのステップを総合することにより，アリスとボブがずれた角度で偏光を測定した場合の可能な相関について詳しく調べた．たとえば，三つの異なる角度 α，β，γ，について次のような不等式

$$N(1_\alpha, 1_\beta) \leq N(1_\alpha, 1_\gamma) + N(1_\beta, 0_\gamma) \tag{1.24}$$

が成り立つ [28]．ここで

$$N(1_\alpha, 1_\beta) = \frac{N_0}{2}\cos^2(\alpha - \beta) \tag{1.25}$$

はアリスが方向 α に偏光角度を設定して “1” を得ると同時に，ボブが方向 β に偏光角度を設定して “1” を得る確率，N_0 は粒子源から放出された粒子ペアの数である．もし角度を，たとえば $\alpha - \beta = \beta - \gamma = 30°$ に選ぶならばこの不等式は破られる．この不等式の破れは，ベルの不等式を導いた仮定の少なくとも一つは量子力学と両立しないことを意味する．通常，それは量子力学の非局所性の現れと見なされている．それが非局所性を説明する唯一のものというわけではないが．

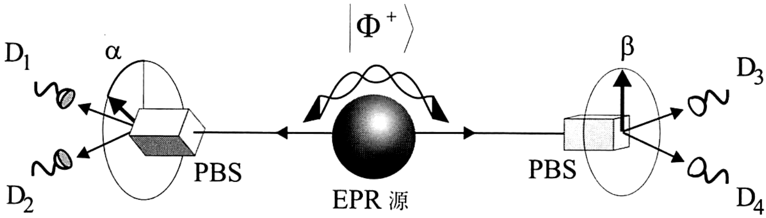


図 1.8 アリスとボブが異なる測定基底を選択した場合（偏光ビームスプリッタ PBS の設定角度 α と β が異なるとき），アリスとボブの測定結果間の相関がベル不等式の破れを導く

1.8 おわりに

この章で議論してきたようなことは10年ほど前は哲学的な議論と思われてきた．もちろん，それはわれわれを取り巻く世界やそこにいるわれわれの役割について理解するための試みと密接な関係があるのではあるが．しかしここ数年，この分野の創成期の研究者達にすら大きな驚きであるが，重ね合わせの原理とエンタングルメントは新しい量子通信と量子計算のスキームにおいて鍵となるものであることが明らかになってきた．この章は要約的なイントロダクションに過ぎない．詳細は本書のそれぞれの章を参照されたい．さらにはウェブページでもいろいろ詳細な知見を得ることができる．たとえば，www.qubit.org や www.quantum.at およびそこから張られた関連リンクを参照されたい．

第2章

量子暗号

(*A. Ekert, N. Gisin, B. Huttner, H. Inamori, H. Weinfurter*)

2.1 古典暗号の何が問題なのか？

2.1.1 SCYTALE から ENIGMA へ

他人に内緒で情報交換をしたいという要望が人類に芽生えたのは，少なくとも文字の発明と同じくらい古く，文明の黎明期にまでさかのぼる．秘匿通信の手法は，メソポタミア，エジプト，インド，中国をはじめとする多くの古代社会で開発されたが，暗号学[1]の起源の詳細はよくわかっていない [29].

ヨーロッパにおいて，軍用暗号の先駆けになったのは，ギリシャ文明の中でも最も好戦的であったスパルタ人である．紀元前 400 年頃から，彼らは SCYTALE という装置を使っていた．司令官たちが情報交換に用いたこの装置は，羊皮紙や皮をテープ状にしたものにメッセージを載せて，先細の棒に螺旋状に巻き付けたものである．文章は，棒の縦方向に，ちょうど 1 文字 1 文字がテープのひと巻に載るように記入する．テープを棒からをほどくと，メッセージの文字はバラバラに見えるので，このほどいたテープだけを先方へと届ける．メッセージの受け手が，このテープをまったく同じ形をした棒に巻き付けると，もとのメッセージが図 2.1 のように浮かび上がってくる．

[1] 秘匿通信の学問は,「隠れた」を意味するギリシャ語の *kryptos* と,「言葉」を意味する *logos* から，英語で cryptology と呼ばれる．cryptology には，暗号を作る技術である cryptography と，暗号を解読する技術である cryptanalysis が含まれる．

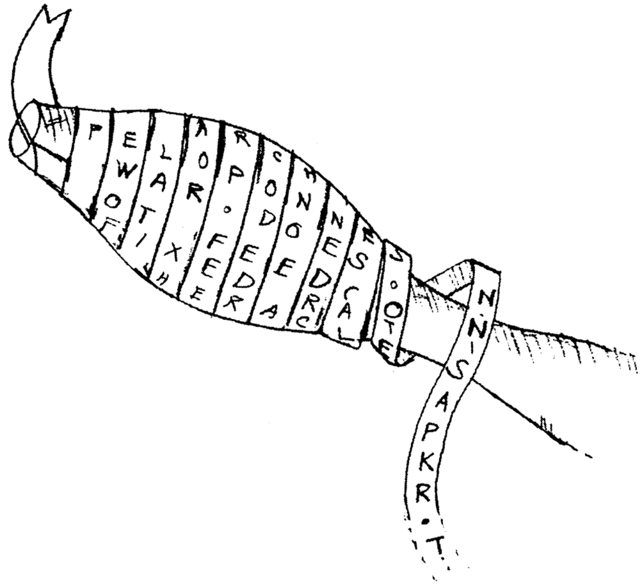


図 **2.1**　最初の暗号機 SCYTALE

ユリウス・シーザーは，文書のやり取りの際に，簡単な換字法を使っていたと言われている．シーザーの方法では，メッセージの各文字を，アルファベット順で三つ後ろの文字に置き換える．つまり，A は D に置き換えて，B は E に置き換えて，という具合である．たとえば，COLD という英単語をシーザー置換すると，FROG になる．この方法は，置換のときにずらす大きさが 3 以外の場合も含めて，今でもシーザー暗号と呼ばれている．

以上二つの簡単な例には，実は，現代の暗号でも用いられている二つの基本的な暗号化の手法，すなわち転置法 (transposition) と換字法 (substitution) が含まれている．転置法（例：SCYTALE）では,「平文」（plaintext; 送りたいメッセージのこと）の各文字を決まった置換規則によって並び替える．換字法（例：シーザー暗号）では，平文の各文字を別の文字，あるいは数字や記号に置き換える．一般には，この二つの手法は組み合わせて同時に使うことができる．

高度な暗号は，ついこの間まで，主に軍事利用に限られていた．第 2 次世界大戦中ドイツ軍で広く用いられた有名な暗号機 ENIGMA や，米軍の暗号

機 M-209 のような複雑な機械を作れる力があったのは，軍機関だけであった．ENIGMA 暗号は，ポーランドで大戦前に解読され，イギリスのブレッチリー・パークでも大戦中に解読された．ブレッチリー・パークの解読チーム（Alan Turing もその一員である）は，暗号の解読のために電気式の機械の開発を行い，最初のデジタル計算機である COLOSSUS を作った．このように，現代暗号（文献 [30]-[32] などを参照）と計算機科学は時を同じくして誕生した．有名な RSA 公開鍵暗号の発明者の一人である R. L. Rivest は，暗号解読は「計算機科学の産婆役」を果たしたと述べている．

2.1.2 鍵とその分配

初期の暗号における暗号文の秘匿性は，暗号化から復号化までを含めた全過程が秘密になっていることに基づいていた．しかし，今日用いられている暗号では，暗号化や復号化のアルゴリズムは秘密にする必要はなく，誰かに知られても暗号文の秘匿性には影響がない．そのような暗号では,「鍵」(key) と呼ばれる一組の変数が平文とともに暗号化のアルゴリズムに入力され，復号化のアルゴリズムにおいても暗号文とともに鍵が入力される．このことは，平文を P，暗号文を C，暗号鍵を k，そして $\hat{E}$ と $\hat{D}$ をそれぞれ暗号化と復号化の操作とすると，次のように書ける．

$$\hat{E}_k(P) = C, \quad \hat{D}_k(C) = P \tag{2.1}$$

暗号化と復号化のアルゴリズムは公開されており，暗号文の秘匿性はひとえに鍵の秘匿性に依っている．この鍵は,「ランダムに選ばれた」十分に長いビット列でなければならない．以上の過程を理解する早道として，別名使い捨てパッド方式 (one-time pad) とも呼ばれる Vernam 暗号を例に挙げよう．

簡単のため，大文字のアルファベットといくつかの句読点だけを使うこととし，それらを以下のように数値化する：

A	B	C	D	E	…	…	X	Y	Z		?	,	.
00	01	02	03	04	…	…	23	24	25	26	27	28	29

秘密鍵暗号の手続きを，次の簡単な例（007 がカクテルを注文する際のセリフ）で見てみよう．

S	H	A	K	E	N		N	O	T		S	T	I	R	R	E	D
18	07	00	10	04	13	26	13	14	19	26	18	19	08	17	17	04	03
15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07
03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10

暗号文（最下行の数字の列）を求めるには，平文の数字（一番上の数字の列）に，0 から 29 までの数字からランダムに選んだ鍵（真ん中の数字の列）を加え，30 で割った余りをとる，すなわち，30 を法とした足し算を行う．たとえば，セリフの最初の文字 “S”は，平文の数字 18 となり，鍵を足すと $18+15=33; 33=1\times 30+3$ となって，暗号文の数字は 3 となる．暗号化と復号化はそれぞれ $P+k (\mathrm{mod}\ 30)=C$，$C-k (\mathrm{mod}\ 30)=P$ と書ける．

この暗号は，1917 年に，アメリカのベル研究所員 Gilbert Vernam によって発明された．後に，Claude Shannon によって，鍵がまったくランダムで，平文と同じ長さをもち，鍵の再利用はしないという条件のもとでは，この使い捨てパッド方式は完全な秘匿性をもつことが示された [33]．さて，このように解読不可能な暗号法があるのならば，古典暗号のいったい何が問題なのだろうか？

実は，落とし穴が一つある．それは鍵分配 (key distribution) の問題である．鍵が使用可能であれば，メッセージの送信に必要なのは，暗号文を通信路を通して送ることだけであり，その通信路は，受動的な盗聴を完全に許してしまってもかまわない．マスメディアを通じて公開してしまう場合などがその一例である．この段階では，確かに解読の危険性はまったくない．しかしながら，もし送受信者の二人が最初秘密の情報をまったく共有していない状態から始めるとすると，使用可能な鍵を手にするためには，通信の手続きのどこかで，信頼のおける秘匿性の高い通信路を使用しなければならない．盗聴行為は，盗聴者が通信路に対して行う一連の測定であるから，古典的に鍵が分配されている場合，正規の利用者に盗聴行為を気づかれることなく通信内容を受動的に傍受することは，技術的な見地からは困難だとしても,「原理的には」可能である．もしも，いったん鍵を手にすることができればそれがずっと使えるという話であったならば，こういった点はたいして問題にはならないだろう．その場合，たとえば強固な金庫を厳重に監視するなどの方法で，鍵が相手の住所まで安全に届くよう十分な対策を講じればよい．ところが，実

際はメッセージを送るたびに新しい鍵が要るということなので，そのような鍵の分配法はえらく高価なものになってしまう．この理由で，大抵の場合には，絶対的な秘匿性はあきらめて，安価で秘匿性の低い方法に甘んじることになる．

より日常的な場面での通信では，DES(Data Encryption Standard) がちょうどよい選択肢である．DES は 1977 年に制定され，機密ではないが慎重を要する情報，とくに商取引などで今でも使用されている．この暗号システムでは非常に短い鍵が使われ，その長さは 64 ビットで，そのうち 56 ビットが直接アルゴリズムに使用され，残りの 8 ビットはエラー検出用である．平文は 64 ビットのブロックに分けて暗号化される．一番簡単な実装法の場合は，長い平文をブロックに分割して，各ブロックを鍵を用いて暗号化する．より複雑な（秘匿性の高い）方法では，各ブロックの暗号化がそれより前のブロックに依存するようにして，暗号を強化する．DES が解読されたとの噂がしばしば流れているが，実証されたものはなく，どうやら DES は優れた基準に基づいて設計されており，鍵の短さからいえば非常に優れたアルゴリズムと言えそうである．DES の多様な可能性についてのさらなる議論は，この解説の主旨を外れるので，他の文献やインターネットを参照されたい．前に述べたように，これらの手法はどれも秘匿性が完全ではない．同一の鍵が何度も使用されるため，暗号文には平文の情報が残されている．暗号化手法の目標は，その情報をできる限りうまく隠すことである．暗号解読の専門家が専念すれば，暗号を解読して平文を取りだすことは可能だろうが，解読に長時間を要すれば，そのときには情報自体が古くて価値がないということもありうる．多くの場合，一つの鍵の使用は数日に留めて，新しい鍵に入れ替えることが推奨されている．もちろん，鍵を受信者にどう送り届けるかという問題はやはり残るのだが，実際上は，必要とされる鍵の長さが非常に短くなれば，その問題はそれほど深刻にはならない．

以上のように，かなりよい秘匿性が実現可能なわけだが，それでは完全な秘匿性はどうだろうか？　前に述べた簡単な議論によれば，鍵分配の問題さえ解決されれば，あとは使い捨てパッド方式によって原理的には完全な秘匿性をもつ通信が達成できる．問題は，鍵分配における問題を解決することができるか？ということになる．その答えは，基本的にはイエスである．非常に興味深い解決法が二つあって，一つは数学的，一つは物理的な解決である．

数学的なものは公開鍵暗号 (public-key cryptography) として知られ，物理的なものは量子暗号 (quantum cryptography) と呼ばれている．

2.1.3　公開鍵および量子暗号

話を進める前に，三人の主要な登場人物を紹介しておこう．アリス (Alice) とボブ (Bob) の二人が，内緒で通信をしたいと考えており，もう一人のイブ (Eve) が盗聴者 (eavesdropper) である．話の筋書きはこうである．アリスとボブは秘密鍵を作りたい．一方，イブのほうは，その鍵についての情報を部分的でもよいから手に入れたい．

暗号研究者たちは，アリスとボブがこのゲームに勝つように，つまり鍵分配の問題を解決するべく，努力を重ねてきた．たとえば，1970 年代に登場したのが，公開鍵システムという巧妙な数学的発見である．今日では，Diffie-Hellman 鍵交換プロトコル [34] と RSA 暗号システム [35] の二つの公開鍵暗号手法が主に使用されている．この二つは，学術界ではそれぞれ 1976 年と 1978 年に発見された．しかし最近になって，英国政府機関はそれ以前からこれらの手法を知っていたことを公式に認めている．実際，これらの手法の先駆けとなったのは，CESG（英国電子通信安全局）の James Ellis によって 1970 年代初期に発見された "Non-Secret Encryption" と呼ばれる技術である．1973 年には，Ellis のアイデアに基づいて C. Cocks が今の RSA に相当する手法を開発し，1974 年には M. Williamson が今の Diffie-Hellman 鍵交換プロトコルと本質的に同じものを提唱している．

公開鍵システムでは，利用者はメッセージを送信する前に秘密鍵を共有する必要はない．この手法の原理は，二つの鍵をもつ金庫であり，一つは施錠のための公開鍵 (public key)，もう一つは解錠のための秘密鍵 (private key) である．施錠する鍵は誰もがもっているのだが，解錠できる鍵をもつのはただ一人なので，メッセージを金庫に入れることは誰でもできる一方，それを取りだせるのは一人だけである．別のアナロジーとしては，図 2.2 に示したような，南京錠の例がある．公開鍵システムは，ある種の数学的操作は順方向が逆方向よりも簡単であるという事実を利用している．このシステムは，鍵分配の問題は回避できるものの，残念ながらその秘匿性は，大きな数の因数分解は難しいといった，証明されていない数学的な仮定に依存している．要するに，公開鍵から秘密鍵を導き出すことは必ずできるはずなのだが，その

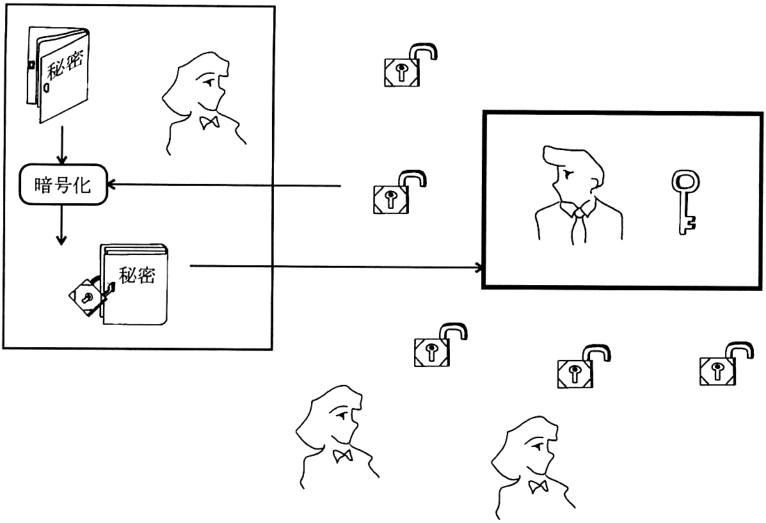


図 2.2 公開鍵暗号システムは次のような機械的なアナロジーで説明できる．ボブは南京錠をたくさん作ることができて，ボブに秘密のメッセージを送りたい人は誰でもボブの作った南京錠を手に入れることができるとしよう．開いた南京錠は，公開鍵に対応する．南京錠を手にしたアリスが，南京錠をひとたび閉じると，それを開けられるのは，南京錠の鍵（秘密鍵）をもっているボブだけである．したがって，アリスは，ボブに送りたいデータを何でもこの南京錠でロックすればよい．ロックされたデータは，ボブだけが手持ちの秘密鍵で取りだすことができる

導出が難しいのだ．たとえば，RSA 暗号（Ron Rivest，Adi Shamir，Leonard Adleman [35] の三人の発明者の名前をとった，広く普及している公開鍵暗号システム）では，大きな数の因数分解の困難性が暗号の秘匿性を生んでいる．数学者たちは，N 桁の数を因数分解するのに必要なステップ数は，どんな古典計算機でも N に対して指数的に増加する，すなわち，因数分解する数を一桁大きくするごとに，計算時間は定数倍になると（証明はされていないものの，固く）信じている．そうであれば，桁数を増やしていくと，因数分解の計算はたちまち手に負えないものになる．

このことは，もし数学者や計算機科学者が大きな数を因数分解する速くて巧妙な手続きを思いついてしまったら，そのときには，公開鍵システムの秘匿

性や安全性はすべて一夜にして消し飛んでしまうことを意味している．実際，量子計算の最近の研究によれば，少なくとも原理的には，量子コンピュータは古典コンピュータよりもはるかに速く因数分解を行えるのである [36]！　ということは，ある意味では，公開鍵システムはすでに安全ではなくなっている．RSA 暗号を用いて今日記録されたメッセージは，最初の量子コンピュータのスイッチがオンになるや否や解読可能になってしまうわけで，その幸せな日になってもまだ秘密にしておきたい情報には，RSA 暗号は使えない．確かに，その日はおそらくは何十年も先のことであろう．しかし，誰がそうだという証明あるいは確かな保証を与えられるだろうか？　今の RSA システムが秘匿性のよりどころとしているものは，技術進歩は遅いという信念だけなのである．

量子暗号は，鍵分配の問題を解決するまったく新しい方法である．量子計算は，その片手で取り上げてしまったものを，少なくとも部分的にはもう片方の手で返してくれているのだ．量子計算のうちで最も簡単な部類の一つが，今日実験室で繰り返し実行され，おそらくすぐに製品として企画されるであろう量子暗号なのである．量子暗号は，完全な秘匿性をもつ鍵の分配を提供する．なぜなら，あらゆる古典暗号とは異なり，量子暗号は，盗聴するには計算時間がかかりすぎるといった仮定ではなく，物理法則をよりどころにしているからである．

量子暗号について詳しく述べる前に，秘匿通信において生じるもう一つの問題，すなわち「認証」(authentication) について簡単に触れておこう．

2.1.4　認証：シンデレラを見分けるには？

ここまでの話では，通信路（チャンネル）に対して不正な介入はないものとしていた．すなわち，アリスとボブの間で交わされる通信内容をイブが傍受することはあっても，イブがそれを偽造したり改ざんしたりすることはできないと暗に仮定していた．言い換えると，アリスとボブは完全な公開チャンネルを使用できるという仮定で，ここで公開チャンネルとは，ラジオ放送のように，誰でも自由に傍受できるけれども，送信される情報を改変することはできないような通信路を指す．多くの現実的な状況下では，こう仮定してしまうのは危険であろう．場合によっては，頭のいいイブはアリス－ボブ間の通信路を二つに切って間に入り込み，ボブにはアリスのふりをして話か

け，アリスにはボブのふりをして話をしてくるかもしれない．

この場合，イブは，たとえば公開鍵と秘密鍵の組を二組作り，公開鍵の一方をアリスに渡して，それがボブの公開鍵だと思わせることができる．もう一方の公開鍵は，アリスの公開鍵だと思わせてボブに渡す．対応する二つの秘密鍵はイブの手もとに残しておくと，それ以降のアリスとボブの間の通信は，完全にイブの思いのままになってしまう．

同じように，使い捨てパッド方式のような秘密鍵暗号システムも，送ったメッセージが敵に知られていると改ざんを防げなくなる．たとえば，ある大使館が前述の Vernam 暗号を用いて母国と通信するとしよう．もし送られているメッセージ，たとえば人物の名前などをイブが正確に知っているとすると，イブはまず，暗号文を途中で横取りして，目的地に届かないようにする．ここで，暗号文からメッセージを 30 を法として引き算すると，そこで使われている Vernam 鍵が手に入る．その後は，偽情報を流すなどおもしろい目的のためにイブはこの鍵を好きに使うことができる．この例でわかるように，たとえ完全な秘匿性をもつ暗号システムであっても，やみくもに使うべきではない．

公開鍵の認証や，メッセージの認証は，上に述べた類いの攻撃（中間一致 (man-in-the-middle) 攻撃とか世界分離 (separate worlds) 攻撃と呼ばれている）に対抗する暗号技術である．

アリスとボブが，ちゃんと秘密鍵を共有してしまえば，簡便で効率的に認証を行う方法がある．しかし，今のところ，公開鍵を認証する簡単な方法はない．鍵が本物かどうか確実にチェックするには，所有者と直接会うしかない．残念ながら，量子鍵分配も，中間一致攻撃に対してはもっと簡便な認証法を新たに提供してはくれない．アリスとボブは，認証用の鍵を交換するために少なくとも一度は顔を合わせる必要がある[2]．

次節以降では，アリスとボブは，完全な公開チャンネルを使用できると仮定する．ただし，認証の問題についても，ごく短くではあるが後で立ち戻ることにしよう．

---

[2] どちらの場合でも，アリスとボブは，第三者，すなわちデジタル鍵の認定を受けもつ信用のおける認証機関に頼ることもできる．

2.2　量子鍵分配

量子鍵分配についての議論の手始めとして，一般的な原理をいくつか概観する．その後，より詳細な説明を加え，2.6 節では実験について考察する．

2.2.1　はじめに

量子鍵分配では，まず，単一粒子あるいはエンタングルした粒子をアリスとボブの間で伝送する．盗聴行為は，物理的な見方をすると，情報の担い手（この場合には伝送されている粒子）に対して盗聴者が行う一組の測定により構成されている．量子力学のルールによれば，一般には，イブがどんな測定をしても，送られている粒子の状態はどうしても変化してしまうので，後でアリスとボブは公開チャンネルでの通信でこれを発見することが可能である[3]．このように，量子鍵分配システムの主な構成は，粒子をやりとりするための量子チャンネルと，量子チャンネルでの伝送が正しく行われたかどうかの検証に用いるいわゆる公開チャンネルである（図 2.3）．繰り返しになるが，公開チャンネルは，誰でも自由に傍受できるけれども，送信される情報を改変することはできないものとしている．

量子伝送の際に鍵がどうなっているかというと，単一粒子の場合は，あらかじめ決めておいた非直交な量子状態の組を使って鍵が符号化されている．エンタングルした粒子の場合は，伝送したあとで，あらかじめ決めておいた一組の測定の結果から鍵を生成する（こちらの場合は，伝送時には鍵は存在すらしていない）．

2.2.2　非直交状態の秘匿性：ノークローニング (no-cloning) 定理

秘密の情報を符号化するのに非直交な量子状態を使うというアイデアは，コピーによって偽造することができない「量子マネー」[37] を提唱した Stephen Wiesner によるものである．このからくりは，非直交な量子状態を（あるい

---

[3] ここで，量子力学のルールが正しいとどうして確信できるのか？という疑問が生じるのはもっともである．答えて言うならば，量子力学は非常に高い精度で繰り返し検証されてきており，現時点でわれわれが手にしている中で最良の理論である．一般に物理法則を，特に量子力学の法則を証明してほしいと物理学者に頼んでも，それは大して意味をなさない．当然ながら，量子力学と符合する実験的証拠を集めても，量子力学がより「正しく」なるなどということはないが，たった一つの実験が，理論を否定してしまうことはありうる．われわれの科学的知識が増えていく過程は，仮説と反駁に基づいており，おそらくは量子力学も最終的には新しい理論に取って代わられるだろう．しかし，その新しい理論が，量子力学を現在応用している範囲内に新しい結果をもたらすということはありそうもない．むしろ，新しい効果は，たとえば強い重力場中のような極端な状況下で見つかるだろう．

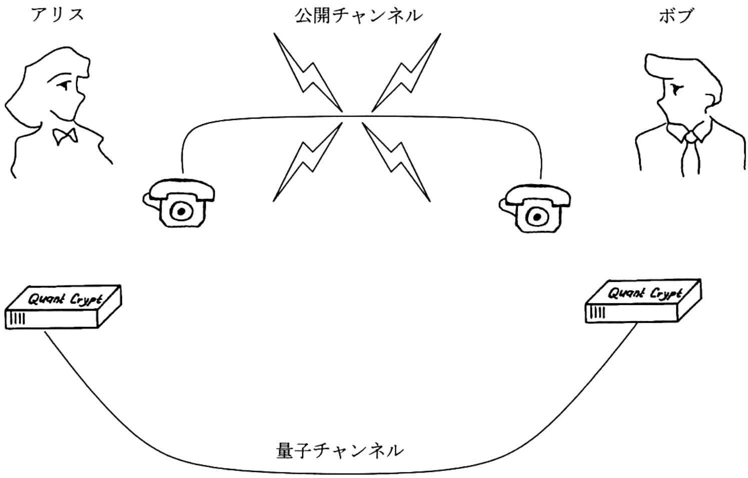


図 **2.3** 量子鍵分配．アリスとボブは，量子チャンネルと古典公開チャンネルの二つの通信路で結ばれている

はどんな未知の量子状態も）複製することができない点にある．このことを見るのに，二つの規格化された状態 $|0\rangle$ と $|1\rangle$ を考え，$\langle 0|1\rangle \neq 0$ としよう．次式のように動作する複製機械が存在すると仮定する．

$$|0\rangle|\text{空}\rangle|\text{機械}\rangle \rightarrow |0\rangle|0\rangle|\text{機械}_0\rangle \tag{2.2}$$

$$|1\rangle|\text{空}\rangle|\text{機械}\rangle \rightarrow |1\rangle|1\rangle|\text{機械}_1\rangle \tag{2.3}$$

ここで「空」は，動作完了後にコピーになる粒子のある初期状態を表し，すべての状態は正しく規格化されているとする．この過程はユニタリでなければならず，内積は保存されるので，必要条件として

$$\langle 0|1\rangle = \langle 0|1\rangle\langle 0|1\rangle\langle \text{機械}_0|\text{機械}_1\rangle \tag{2.4}$$

を得る．この式が成立するのは，$\langle 0|1\rangle = 0$（2 状態は直交）か，$\langle 0|1\rangle = 1$（2 状態は峻別不可能で，したがって二つの異なるビット値の符号化には使えない）の場合だけなので，われわれの最初の仮定と矛盾する．したがって，もし誰かが $|0\rangle$ と $|1\rangle$ をランダムに選んで，$|1\rangle|0\rangle|1\rangle|1\rangle\cdots$ といったランダムな状態の列を密かに用意したとすれば，この列を忠実に複製することは不可能であ

る．こうした複製不可能な量子署名を用いた Wiesner のマネーは，非直交な量子状態を通帳に保存しておくことを必要とするが，これは非直交な量子状態をある場所から別の場所に送るよりもはるかに難しい．そのようなわけで，Wiesner のアイデアは鍵分配に応用されることとなった．Charles Bennett と Gilles Brassard の提案では，暗号鍵の分配に偏光した光子の非直交な状態が用いられる [38]．量子チャンネルで送られている非直交な $|0\rangle$ と $|1\rangle$ を盗聴者が区別しようとすると，どうしても問題が生じる．仮定として，イブは自分の測定装置を最初規格化された状態 $|\mathrm{m}\rangle$ に準備し，$|0\rangle$ と $|1\rangle$ をこの 2 状態を乱すことなく見分けたいとしよう．つまり，イブは次のようなユニタリ変換を実行したい．

$$|0\rangle|\mathrm{m}\rangle \to |0\rangle|\mathrm{m}_0\rangle \tag{2.5}$$

$$|1\rangle|\mathrm{m}\rangle \to |1\rangle|\mathrm{m}_1\rangle \tag{2.6}$$

ユニタリという条件から，$\langle 0|1\rangle\langle \mathrm{m}|\mathrm{m}\rangle = \langle 0|1\rangle\langle \mathrm{m}_0|\mathrm{m}_1\rangle$，すなわち $\langle \mathrm{m}_0|\mathrm{m}_1\rangle = 1$ となって，測定装置の終状態はどちらの場合も同じである．二つの状態は乱されないが，イブは符号化されたビットの値について何ら情報を得られない．より一般的な測定（ただし最も一般的なものではない）として，もとの状態を $|0\rangle \to |0'\rangle$ および $|1\rangle \to |1'\rangle$ というように乱すものは，次の形に書かれる．

$$|0\rangle|\mathrm{m}\rangle \to |0'\rangle|\mathrm{m}_0\rangle \tag{2.7}$$

$$|1\rangle|\mathrm{m}\rangle \to |1'\rangle|\mathrm{m}_1\rangle \tag{2.8}$$

ユニタリ条件から，$\langle 0|1\rangle\langle \mathrm{m}|\mathrm{m}\rangle = \langle 0'|1'\rangle\langle \mathrm{m}_0|\mathrm{m}_1\rangle$ となる．$\langle \mathrm{m}_0|\mathrm{m}_1\rangle$ が最小になるときが，イブが 2 状態をもっともよく見分けられる場合に相当するが，それは $\langle 0'|1'\rangle = 1$，すなわち $|0\rangle$ と $|1\rangle$ が相互作用の後で同じ状態になってしまう場合である．ここで例に挙げた測定は最も一般的なものとは言えないものの，測定によって得られる情報と，もとの状態の擾乱との間のトレードオフをよく表している．このトレードオフを利用した鍵分配プロトコルについては後で詳しく述べよう．

2.2.3　エンタングルメントの秘匿性

エンタングルメントに基づいた量子暗号の着想の根底にあるのは，今までの話とは別のもので，Einstein-Podolsky-Rosen のパラドクスに関係がある．

1935 年に，Einstein は Boris Podolsky と Nathan Rosen とともに (EPR) 論文を出版し，その中で，自然の「妥当な」基礎理論はどうあるべきかについて述べた [21]．この EPR の規範では，完全性（「完全な理論は，実在の各要素に対応して一つの要素をもつ」）と局所性（「系 A の実在としての状態は，空間的に離れた時空における系 B に対する操作とは独立である」）が必要とされ，物理的実在の要素は次のように定義された──「もし，まったく系を乱すことなく，ある物理量の値を確実に予言できるとき，この物理量に対応した物理的実在の要素が存在する」．続いて，彼らはエンタングルした 2 粒子に対する思考実験を考え，量子状態があらゆる状況で物理的実在の完全な記述を与えるということはありえないことを示した．EPR の議論を，後に David Bohm が少し変更したものを以下に述べよう [15]．1 重項スピン状態にある二つのスピン 1/2 粒子

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle) \tag{2.9}$$

を考える．ここで，1 粒子ケット $|\uparrow\rangle$ と $|\downarrow\rangle$ はある決まった方向についてのスピン上向きとスピン下向き状態を表す．この状態 $|\Psi\rangle$ は球対称であり，この方向の選び方はどうでもよい．二つの粒子（A と B と呼ぶことにする）は，ある粒子源から飛び出して，互いに遠ざかっていく．十分に距離が離れて 2 粒子が相互作用しなくなったら，粒子 B のスピンの x 方向の成分の測定によって，粒子 A のスピンの x 成分を確実に予言することができる．粒子 B に対して行われた測定は，(局所性によって) 粒子 A を乱さない．したがって，スピンの x 成分は，EPR の基準によれば実在の要素である．$|\Psi\rangle$ が球対称であることから，同じ議論によって，y，z，その他どんな方向のスピン成分もまた実在の要素になる．しかし，スピンのすべての成分が決まった値をもつようなスピン 1/2 粒子の量子状態はないので，量子論の実在の記述は不完全ということになる．

EPR の規範は，量子的実在の別の記述の仕方を要求したが，そのような記述が可能なのか，またもし可能なら，それは異なる実験的予言につながるのかという問題は，1964 年のジョン・ベルの定理が出るまで明らかではなかった．ベルは，エンタングルした粒子にかかわる量子力学の予言で，EPR の主張する局所性，実在，完全性とは相容れないようなものがあることを示した [23]．EPR の規範から実験的に検証可能な不等式が導かれるが，ある量子力

学の予言がその不等式を破ることから，この矛盾が生じる．1.7 節に，この不等式の簡単な導出が述べられている．ベルの定理は 1974 年に John Clauser と Michael Horne によって拡張され，EPR の規範の実験的検証が可能になった [39]．かなりの数の検証実験が行われており，実験結果は量子力学の予言を支持している．

この話がデータの秘匿性とどうかかわりがあるのだろうか？　驚くべきことに，大ありなのである！　量子論の概念の基礎を検証するためにベルが用いた技巧そのものが，データ送信を盗聴者から守るのに使えることがわかったのだ！　ひょっとすると，EPR による実在の要素の定義——「もし，まったく系を乱すことなく，ある物理量の値を確実に予言できるとき，この物理量に対応した物理的実在の要素が存在する」．——を思い起こすと，これはそれほど驚くことではないかもしれない．もしこの物理量を使って暗号鍵のビット値を符号化したとすると，盗聴者の求めるものは符号化に用いた観測量に対応した実在の要素にほかならない．このように，エンタングルメントに基づく量子暗号によって，量子エンタングルメントとベルの定理の実用的な使い道が生まれた．純粋学問的な研究と実際的な研究との境界は，かなり曖昧だということがわかる．プロトコルの詳細については後述する．

2.2.4　雑音のある量子チャンネルの場合は？

量子伝送をどのように行うにしても，結論としては，完全な量子チャンネル（すなわち，雑音のないチャンネル）は秘匿性をもつということになる．通信の乱れはすべて，盗聴者が通信路に割って入ろうと試みた兆候である．したがって，雑音の交じった通信結果はすべて棄却しなければならない．残念なことに，量子チャンネルは非常に脆く，実際には盗聴者とは関係なく環境との相互作用によってある程度は悪意のない雑音が生じるのは避けられない．そこで正規の利用者は，雑音入りの通信結果は何でも捨てるというのではなくて，ある程度の雑音がある場合でも秘密鍵を取りだす手段を見つける必要がある．まず第 1 に，アリスとボブは，測定可能な変数の関数として，どれだけの量の情報が盗聴者に洩れた可能性があるかを見積もらなければならない．この情報量は，問題なしか，許容範囲内か，許容範囲外のいずれかの場合がある．ここで許容範囲内というのは，秘匿性増幅 (privacy amplification) や量子秘匿性増幅（8.4 節を参照）など何らかの追加の手続きによって，鍵の

長さを短くするという代償を払って漏洩情報量を問題のないと思われるレベルまでいくらでも減らすことができる場合を意味する．しかし，あるしきい値があって，あまりに多くの情報が盗聴者に洩れると，秘匿性増幅は不可能になり，通信結果は捨てなければならない．より精密な秘匿性の判断基準の必要性は，はじめ Huttner と Ekert により強調され [40]，以来，量子盗聴は一つの研究分野に成長している．

雑音のあるチャンネルを使った量子伝送が，エンタングルした粒子の配送に基づく場合には，盗聴者が行いうる最も一般的な攻撃を考慮した形での秘匿性の判断基準が，量子秘匿性増幅によって与えられる．量子秘匿性増幅は，(盗聴やその他外部からの干渉の結果) 部分的にしかエンタングルしていない粒子を完全にエンタングルした粒子に変換する．また，どのような場合にそういった量子エンタングルメントの精製が可能なのかもわかっている．しかしながら，実用の観点では，量子精製を行うのに必要な技術は量子計算を行うのに必要な技術に近く，したがって現状ではまだ不可能である．

単一粒子を伝送する場合の秘匿性に関する文献はかなりの数にのぼる．はじめは，いわゆるインコヒーレント (incoherent) 攻撃——イブはアリスの粒子を 1 個 1 個別々に操作する——に対する秘匿性が議論された．しかし，量子力学の範囲では，イブが量子コンピュータを駆使するような，より一般的かつより強力な攻撃も可能であり，コヒーレント (coherent) 攻撃と呼ばれている．そのような攻撃に対する秘匿性の証明は最近になって提出された．ただ，より強力な攻撃を考慮すればするほど，秘匿性のために必要な条件はより厳しいものになってしまう．実際の応用の際に重要な，プロトコル全体の最適化についても同じことがあてはまる．

2.2.5 実現性

量子暗号はいくつか他の問題も抱えている．まず第 1 に，2.4 節で述べるエンタングルした光子対を使う場合を除いて，大抵の実装に共通する問題は，純粋に 1 光子からなるパルスを生成する方法がまだわかっていないという点である．量子暗号の光源は普通，レーザ光を単に減光したものが用いられる．この種の光では，パルス中の光子数はポアソン分布に従うランダムな値をとる．つまり，パルスによっては光子がまったくないこともあれば，1 個，2 個あるいはそれ以上の光子を含むこともある．パルス中に光子が 2 個以上ある

と，盗聴者に情報が洩れる可能性があるので，そういったことは避けなければならない．パルス中に光子が 2 個以上ある確率を十分に低くするには，非常に弱いパルスを使う必要があり，そうすると今度は S/N 比が低下してしまう．よく用いられる値はパルス当たり平均 0.1 光子で（つまり，10 パルスのうちたった 1 パルスが 1 光子を含んでいる），このとき光子が 2 個以上ある確率は 5×10^{-3} である．このレベルでもまだ使える（光子を 1 個以上含む）パルスのうち 5% が光子を 2 個以上含み，盗聴者に情報が洩れる可能性を残すことになる．よい単一光子光源を開発することは，技術的に可能と思われるが，現状ではまだ達成できていない．

2 番めの問題は，量子チャンネルではその量子的性質を保ったまま増幅を行うことはできないという点で，量子暗号を実際に応用する上ではより深刻な問題である．このため，伝送の損失を考え合わせると，量子暗号は限定された距離でしか動作しないことになる．現存するシステムはすべて，シリカファイバで赤外光子を伝送する方式であり，最小の損失レートはおよそ 0.2 dB/km である．だから，100 km（損失 20 dB，あるいは透過率 0.01 になる）を超える距離で量子暗号システムを組むのは，近い将来では無理そうである．したがって，量子暗号による秘匿性を有する大陸間ケーブルなどは，今のところは完全なおとぎ話に留まっている．

3 番めは，量子暗号は 1 対 1 の情報交換にはよく適合するが，それ以外のネットワークにはそれほどうまく適合しないという問題である．最近の提案 [41] によると，この方向でも改善が見られるようだが，それでも一人対数人に限定されている．各家庭を結んだ取引に量子暗号を用いるのも未だ実用的ではない．しかし，ある種の LAN(Local Area Network) で，中央の送信局（たとえば銀行の本店）といくつかの受信局（たとえば銀行の支店）という形態は十分に考えられる．

2.3　単一粒子による量子鍵分配

2.3.1　偏光した光子

偏光した光子による量子鍵分配は，はじめ C. H. Bennett と G. Brassard により提案された [38,42]．その際の実験は，緑色のパルス光を自由空間上で 40 cm 飛ばすもので，これを少し詳しく見ることにしよう．この実験は明らか

に実際の鍵の伝送には使えないが，量子暗号の実験の最初の一歩である．同じプロトコルを約 1 km の光ファイバで実装した実験は，ジュネーブ大学で初めて行われた [43]．最近では，距離は数十キロメートルにまで達している．この節では，偏光した光子による量子暗号の原理について述べ，実験については 2.6 節で述べる．

各パルスが 1 個ずつ光子を含むような，偏光した光パルス列を考えよう．まずは水平か垂直の偏光を考え，量子力学の Dirac の記法でそれぞれ $|\leftrightarrow\rangle$ および $|\updownarrow\rangle$ と書く．情報を送るには何らかの符号系が必要で，たとえば $|\updownarrow\rangle$ が 0 に，$|\leftrightarrow\rangle$ が 1 に対応すると決める．この符号系を使えば，送信者アリスはあらゆるメッセージを受信者ボブに送ることができる．たとえば，もしアリスが $|\leftrightarrow\rangle$，$|\updownarrow\rangle$，$|\leftrightarrow\rangle$，$|\leftrightarrow\rangle$，$|\updownarrow\rangle$ というパルス列を送る場合，対応する 2 進数は 10110 となる．アリスが $|\leftrightarrow\rangle$ と $|\updownarrow\rangle$ のいずれかの状態を送った場合，光子を $\oplus$ 基底で送ったと表現することにしよう．欲しい鍵はランダムであることが必要なので，アリスは 0 と 1 を等しい確率で送信する．メッセージを検出するために，ボブは偏光ビームスプリッタ (PBS) を用いる．これは，垂直偏光はそのまま透過するが，水平偏光は別の方向に出力する．続いて，図 2.4 のように，装置の各出力に単一光子検出器を置く．検出器 D0(D1) での検出は，アリスが 0 を（1 を）送ったことを示す．この場合もやはり，$\oplus$ 基底で検出したと表現することにしよう．検出器は完全ではなく，伝送時にも損失が生じうるので，検出器が両方とも光子を検出しないことがある．その場合，ボブは何も検出できなかったことをアリスに告げ，対応するビットは捨てる．このため，はじめ用意したビット列の一部分しか実際には使われないことになるが，残ったものはアリスとボブで共通の値のはずである．したがって，このシステムは，決まったメッセージを伝送する目的では使えない．しかし，ランダム性と秘匿性だけが要求される暗号鍵の送信には適している．

この段階では，この装置はまったく秘匿性がない．盗聴者イブもボブと同じような装置でパルスを測定し，同じようなパルスを再びボブに送ってやることが可能である．そうすると，イブはアリスとボブが共有したビット値をすべて知ることになる．秘匿性を得るには，アリスはもう一つ別のランダムな選択を行う．すなわち，アリスは先に述べた水平 – 垂直偏光を使用するか，あるいは，二つの斜め直線偏光を $|\swarrow\!\!\!\nearrow\rangle$ なら 0，$|\nwarrow\!\!\!\searrow\rangle$ なら 1 という対応で使用する．後者の場合でも，アリスは 0 と 1 を等しい確率で送信する．これを $\otimes$ 基

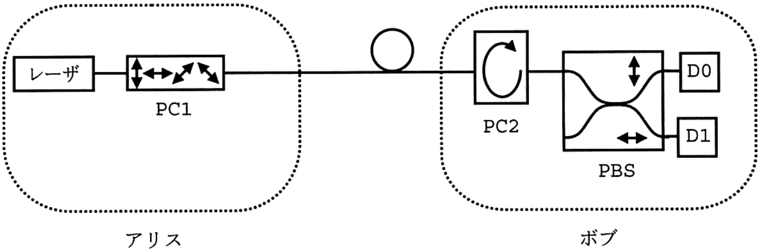


図 2.4　偏光方式：送信者アリスは非常に弱い偏光パルスをボブに送る．偏光はポッケルスセル (PC1) により制御され，アリスは四つの偏光 $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nearrow\rangle$, $|\nwarrow\rangle$ から選択することができる．ボブの側では，もう一つのポッケルスセル (PC2) により測定系の回転角を制御する：0° は ⊕ 基底での測定に対応し，45° は ⊗ 基底での測定に対応する．偏光ビームスプリッタ (PBS) は光を二つの直交する成分に分離し，それらは D0 か D1 で検出される．(図では ⊕ 基底での測定が選ばれている.)

底と呼ぼう．ボブは，装置を 45° 回すことによって，⊗ 基底での測定を選択できる．安全性は，量子力学の基本的な性質，非決定性によって確保される．⊗ 基底で準備された単一光子パルスを ⊕ 基底で測定した場合，光子は 1/2 の確率で D0 か D1 のいずれかの検出器に向かう．しかも，どちらになるかはまったくランダムである．すなわち，光子の中にこれからどちらの検出器に向かうかを示すものは何もない．だから，もしアリスが光子をたとえば状態 $|\swarrow\!\!\!\nearrow\rangle$ に準備して，ボブが（あるいは他の誰かが）それを ⊕ 基底で測定しようとすると，D0 と D1 のどちらが光子をカウントするかは等確率になる．このことは決して，$|\swarrow\!\!\!\nearrow\rangle$ 状態の光子の列のうち半分の光子が垂直偏光で，半分が水平偏光だというわけではないことを強調しておこう．それは，ボブが ⊗ 基底を使った場合はいつでも 0 という結果を得るという事実と矛盾してしまう．実際のところ，この系はあたかも測定されたそのときにどちらのほうへ向かうかをランダムに決めているかのように振る舞うのである．

明らかに，上記の事情はイブにも等しく当てはまる．アリスはランダムにどちらかの基底を使うので，イブは測定の基底をどちらにしたらよいか決められない．間違った基底を使った場合，イブが手にするのはアリスの選択とは何の相関もないランダムな結果である．もう一つ重要なのは，イブは自分が間違った結果を手にしたのかどうか判断がつかないという点である．すな

わち，D0 でカウントがあったら，それは光子が状態 $|\updownarrow\rangle$ に準備されていたことを意味するかもしれないが，同時に，状態 $|\swarrow\!\!\nearrow\rangle$ か状態 $|\nwarrow\!\!\searrow\rangle$ にあった光子が，単に D0 に向かうことを「選択した」という可能性もある．単一光子のパルスを必要とする理由はここにある．すなわち，2 個以上の光子からなるパルスを間違った基底で測定すると，D0 と D1 の両方がカウントする場合があって，イブは自分が間違った基底を選んだことに気づいてしまう．そうしたら，イブは単に送信するのをやめることで，エラーが生じるのを防ぐことができる．しかし，光子が 1 個だけイブのもとに届いたのであれば，イブは測定結果の示す状態に光子を準備してボブに送る以外に選択肢がない．この場合はどうしてもボブの受け取ったビット列の中にエラーを生じることになる．ここで述べた盗聴戦略は，遮断–再送 (intercept-resend) 戦略と呼ばれていて，イブの取りうるいろいろな可能性の中の一つでしかない．

偏光による暗号のプロトコルを構成する基本的な材料はこれで出揃った．一例を表 2.1 に示す．プロトコルの全体の流れは図 2.5 のようになる．概要は以下の通り．

1. アリスは基底と単一光子パルスの偏光をランダムに選んでボブに送る．
2. パルスごとに，ボブもランダムにどの基底を使うか選んでパルスの測定を行う．D0 か D1 でカウントが起こる場合と，検出や伝送での損失のために何もカウントがない場合がある．受信できたビットの集合を未加工鍵 (raw key) と呼ぶ．
3. ボブは公開チャンネルを通じてアリスに，どの光子がカウントされたか，またその際使った基底は何かを告げる．もちろん，ボブの測定の結果（D0 と D1 のどちらでカウントしたか）は告げない．アリスは返答として自分の用いた基底を告げる．$\oplus$ でも $\otimes$ でも，アリスとボブが同じ基底を選んだ場合は両者のビットは完全な相関をもつはずである．しかし，装置には不完全性があり，また盗聴者がいる可能性もあるため，エラーが存在する．この段階のビットの集合を選別済み鍵 (sifted key) と呼ぶ．
4. 一部分食い違いがあり，またおそらく完全には秘匿性をもっていないビット列を，使用可能な共有秘密鍵に変換するために，アリスとボブは何らかの処理を施す必要がある．実は，この処理段階は単一粒子を使う量子暗号のどんな実装にも共通している．主な手続きは次のようなものであ

表 2.1　偏光プロトコルの例．アリスはランダムに基底（$\oplus$ または $\otimes$）とビット値（0 または 1）を選び，対応する偏光状態をボブに送る．ボブもランダムに受信基底を選び，ビット値を得る．この段階のビット列を未加工鍵 (raw key) と呼ぶ．続いて，アリスとボブは公開チャンネルを通じて自分の用いた基底を互いに告げ，同じ基底が使われたときのビット値のみを残す．この段階のビット列を選別済み鍵 (sifted key) と呼ぶ．さらにこのビットの一部分をランダムに選び出し，イブがいたかテストした上で捨てる．この例の場合，エラーは生じていない．つまり，伝送は秘匿性をもつ．残ったビットが共有された鍵となる

A 基底	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
A ビット値	0	1	0	1	1	0	1	0	0	0	0
A 送信	$\vert\nearrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nwarrow\rangle$	$\vert\leftrightarrow\rangle$	$\vert\nearrow\rangle$	$\vert\nwarrow\rangle$	$\vert\updownarrow\rangle$	$\vert\nearrow\rangle$	$\vert\nearrow\rangle$	$\vert\updownarrow\rangle$
B 基底	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
B ビット	0	1	0	0	1	0	1	1	0	1	0
同一の基底？	y	y	n	n	y	y	y	n	n	n	y
A 保持	0	1			1	0	1				0
B 保持	0	1			1	0	1				0
イブは存在？	y	n			y	n	n				n
鍵		1				0	1				0

る．伝送のエラー発生率を見積もる．盗聴者に漏洩した可能性のある情報量の最大値を推定する．すべてのエラーを訂正し，また，イブが利用する可能性のある情報の量を必要とされるレベルにまで落とす．最後に残ったビット列が秘密鍵である．

偏光による方式は，偏光が保存される自由空間では大変魅力的だが，光ファイバでは，減偏光 (depolarization) と複屈折性のランダムな揺らぎのために，実装がより複雑になる．減偏光は大きな問題ではない．この効果は十分にコヒーレントな光源を使うことで抑制できる．安定した条件下での複屈折性の揺らぎの時間スケールはかなり遅い（1 時間）．しかし，敷設したケーブルで実験したところ，はるかに短い時間スケールの揺らぎが観測され，伝送は不

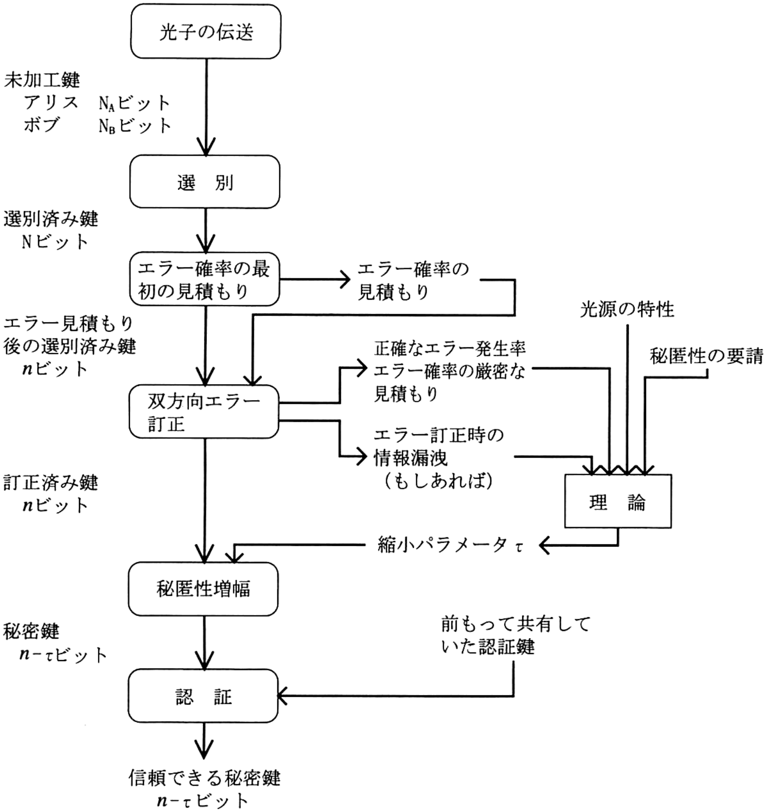


図 2.5　単一光子を用いた量子鍵分配プロトコルの流れ

可能であった．継続的にモニターして偏光を補正する電気的な補償システムは確かに可能であるが，アリスとボブの間でアラインメント調整が必要となる．すると，利用者サイドから見てこの方式はやや面倒に映るかもしれない．

2.3.2　位相符号化システム

光ファイバでは制御の難しい偏光に頼るかわりに，位相による符号化に基づいて量子暗号を作ることもできる．光ファイバとマッハーツェンダー (Mach-Zehnder) 干渉計を使った位相による符号化は，もともとはエンタングルメントに基づく量子暗号の流れで導入されたものだが [44]，単一粒子の方式でも利用可能である [45]．理論上の仕組みを図 2.6 に示す．左側のアリスと右側の

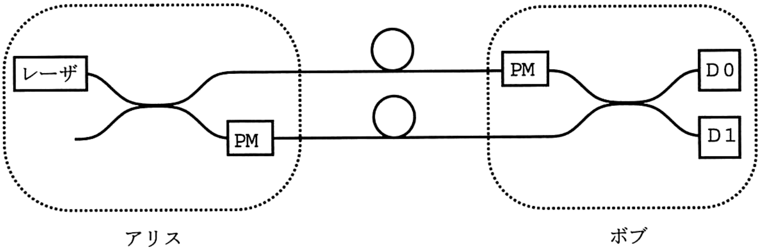


図 **2.6**　引き伸ばしたマッハーツェンダー干渉計による位相方式．二つの位相変調器 (PM) の相対位相の選び方で干渉パターンが定まる．アリスは，⊕ 基底に相当する 0 と π，および，⊗ 基底に相当する $\frac{\pi}{2}$ と $\frac{3\pi}{2}$ の四つの選択肢から選ぶ．ボブは，0（⊕ 基底での測定に相当）か $\frac{\pi}{2}$（⊗ 基底での測定に相当）かを選ぶ．アリスとボブが同じ基底を用いた場合，D0 でのカウントは 0 を意味し，D1 でのカウントは 1 を意味する．二人の基底が異なる場合，アリスの送信したビットとボブの受信したビットの間には相関がない

ボブが2本のファイバで結ばれていて，マッハーツェンダー干渉計を引き伸ばしたものになっている．アリスとボブのどちらの側にも位相変調器 (PM) があって，符号化と復号化が行える．とりあえず，ボブは自分の PM は使わないと仮定して，干渉計は D0 で強め合い，D1 で弱め合うように調整されているとしよう．アリスが自分の PM を使って 0 または π の位相シフト（ビット値 0 と 1 に対応する) を与えると，ボブ側ではそれに応じて D0 か D1 にカウントが起こる．これは前に述べた方式で 2 種類の偏光しか使わなかった場合とちょうど同じである．秘匿性を得るには，ランダムな基底の選択を追加する．この場合だと，アリスは四つの位相シフトから選ぶことになる．つまり，0 と π（⊕ 基底に相当），および $\pi/2$ と $3\pi/2$（⊗ 基底に相当）である．ボブの側でも，位相シフトを 0 にする，すなわち ⊕ 基底で測定するか，位相シフトを $\pi/2$ にする，すなわち ⊗ 基底で測定するかの選択を行う．こうすると，前の偏光方式と等価になる．

残念なことに，このように引き伸ばした干渉計（腕の長さが約 20 km にもなる）において位相差を保つのは非常に難しい．というわけで，より実用的なのは図 2.7 に示したように干渉計を折り畳んだ方式である．アリス側のマッハーツェンダーに 1 個のパルスが入ると，二つのパルスに分割される．1 本の伝送ファイバ中を引き続いて通過するこの二つのパルスを S（短い経路）お

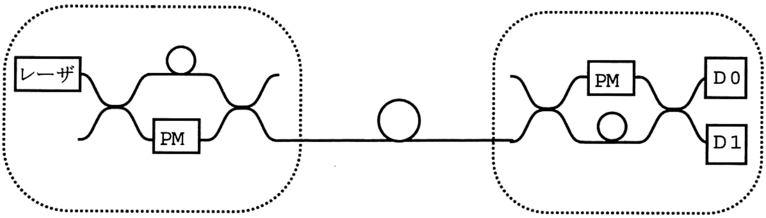


図 **2.7** 折り畳んだマッハ−ツェンダー干渉計による位相方式．二つのパルスは，異なる経路を通るのではなくて，同じ光ファイバを時間差を付けて通る．この方式は干渉計の安定性を増すが，ボブ側の装置に 3 dB の損失が加わる

よびL（長い経路）と表記する．これらのパルスがボブ側のマッハ−ツェンダーを通過すると，出力は三つのパルスになる．そのうち二つ，SS（短い–短い）とLL（長い – 長い）は，干渉効果がないので関係ない．真ん中の出力は，取りうる経路がSLとLSの二つあって，区別できないために干渉が起こる．前の段落と同じように，アリスとボブの位相シフトの選択が符号化と復号化を与える．この方式では，干渉計の大部分で二つのパルスが実際に通る経路が同じなので，前のものよりはるかに安定である．欠点は，信号の半分はSSとLLの経路を通るため無駄になってしまう点である．

C. Bennett が提案した方式 [45] では，アリスの選ぶ位相が 2 種類しかない．詳細については原論文を参照していただきたい．この種のシステムの主な利点は，原理的には偏光の制御が不要なことである．しかし，実際には，部品に偏光特性があるために，偏光も制御したほうがよいようである．さらに，これらの方式でも，干渉計の両端の間で注意深く光路長を調整，制御する必要がある．

2.4 エンタングルした状態による量子鍵分配

2.4.1 未加工鍵 (raw key) の伝送

偏光の 1 重項状態

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle|\leftrightarrow\rangle - |\leftrightarrow\rangle|\updownarrow\rangle) \tag{2.10}$$

にある光子対を生成する光源が備わった量子チャンネルを用いて鍵の分配が行われる．

二つの光子は別々に分かれて，z 軸に沿って，通信路の正規の利用者であるアリスとボブのもとへ飛んでいく．アリスとボブは，光子が分かれた後に，3 種類の基底のうちの一つを選んで測定を行い，測定結果を記録する．ここで，3 種類の基底は，$\oplus$ 基底を z 軸のまわりにアリスは角度 $\phi_1^a = 0$，$\phi_2^a = \frac{1}{4}\pi$，$\phi_3^a = \frac{1}{8}\pi$，ボブは角度 $\phi_1^b = 0$，$\phi_2^b = -\frac{1}{8}\pi$，$\phi_3^b = \frac{1}{8}\pi$ で，それぞれまわして得られるものである．

上付きの添字「a」と「b」はそれぞれアリスとボブの測定装置を表している．二人は，自分の基底をランダムに，しかも送られてくる粒子対ごとに独立に選ぶ．各測定では，起こり得る結果は $+1$（選択された基底の 1 番めの偏光状態に光子が観測された場合）と -1（選択された基底のもう一方の偏光状態に光子が観測された場合）の 2 種類あって，最大 1 ビットの情報が提供される．

アリスが ϕ_i^a 回転した基底を用い，ボブが ϕ_j^b 回転した基底を用いて測定したときの相関係数を

$$E(\phi_i^a, \phi_j^b) = P_{++}(\phi_i^a, \phi_j^b) + P_{--}(\phi_i^a, \phi_j^b) - P_{+-}(\phi_i^a, \phi_j^b) - P_{-+}(\phi_i^a, \phi_j^b) \quad (2.11)$$

とする．ここで，$P_{\pm\pm}(\phi_i^a, \phi_j^b)$ は，ϕ_i^a で指定される基底で結果 ± 1 が得られ，ϕ_j^b で指定される基底で結果 ± 1 が得られる確率を表す．量子論によれば

$$E(\phi_i^a, \phi_j^b) = -\cos[2(\phi_i^a - \phi_j^b)] \quad (2.12)$$

である．二人の装置が同じ方向になる基底の選び方が 2 種類（ϕ_1^a, ϕ_1^b と ϕ_3^a, ϕ_3^b）あるが，その場合，量子力学はアリスとボブの得る結果が完全な反相関をもつことを予言する．すなわち，$E(\phi_1^a, \phi_1^b) = E(\phi_3^a, \phi_3^b) = -1$ である．

アリスとボブの測定装置の方向が異なる場合の相関係数から，次のように量 S を定義する．

$$S = E(\phi_1^a, \phi_3^b) + E(\phi_1^a, \phi_2^b) + E(\phi_2^a, \phi_3^b) - E(\phi_2^a, \phi_2^b) \quad (2.13)$$

これは，Clauser，Horne，Shimony，Holt によって提出された一般化されたベルの不等式，いわゆる CHSH 不等式 [12] における S と同じものである．量

子力学の要請は

$$S = -2\sqrt{2} \tag{2.14}$$

である．

光子の伝送が完了したら，アリスとボブは，それぞれの測定において選択した測定装置の方向を公開し，一連の測定を二つのグループに分ける．第1のグループは，二人が異なる測定装置の方向を選んだ場合で，第2のグループは，測定装置の方向が同じ場合である．二人のいずれか，あるいは両方が，粒子の到達を記録していないケースは，すべて破棄する．続いて，アリスとボブは，第1のグループに属する測定結果のみを公開する．これにより，二人は S の値を決定することができる．もし，粒子が直接にしろ間接にしろ干渉を受けなかったとすれば，式 (2.14) の結果が再現されるはずである．この結果が得られれば，正規の利用者である二人は，第2のグループに属する測定結果が反相関をもち，秘匿性をもつビットの列，すなわち鍵に変換できることを確信できる．

盗聴者イブは，光源から正規の利用者へと伝送される粒子からは，何の情報も引きだすことができない．理由は単純で，そこには何の情報も載っていないからである！　正規の利用者が測定を行い，後に公開チャンネルで交信して初めて，情報が「生まれでる」のである．イブは，アリスとボブの粒子を自分で用意したデータにすり替えることによって，彼らを出し抜こうと試みるかもしれないが，各粒子対に対して測定装置のどの方向が選択されるかはイブにはわからないので，盗聴の露見を免れるうまい戦略はない．この場合，イブによる干渉は，偏光方向について「物理的実在」を導入することと等価であり，S の値を「量子的な」値よりも小さくしてしまう．というわけで，実に，ベルの定理で盗聴者をあぶり出すことが可能なのである．

2.4.2　秘匿性の判断基準

このシステムにおける盗聴を解析する最良の方法は，盗聴に最も有利なシナリオ，すなわち，アリスとボブが鍵を作るのに用いる粒子対をイブ自身が用意するケースを考えることである．チャンネルに生じる雑音は，（すべてではないにしても）ほとんどがおそらく罪のない環境からの雑音なのだが，上のシナリオでは，すべての雑音の原因を盗聴に帰するという，最も控えめな立場に立つことになる．

盗聴の解析の手始めとして，ベルの定理の精神に則って，どの粒子がどの状態にいるかをイブが正確に把握しているという単純な場合を考えよう．文献 [46] に従い，EPR 対の 2 粒子をイブが別々に準備して，対になる二つの粒子それぞれがはっきりと決まった偏光方向をもつと仮定しよう．この方向は，対ごとに異なっていてもよい，つまり，イブは確率 $p(\theta_a, \theta_b)$ でアリスの粒子を状態 $|\theta_a\rangle$ に，ボブの粒子を状態 $|\theta_b\rangle$ に準備する．ここで，偏光を指定する θ_a と θ_b は，垂直軸から測った角度である．このような準備の仕方の場合，イブは，1 粒子 1 粒子それぞれの状態を自由に制御していることになる．この場合，イブは常に優位に立つので，アリスとボブは鍵を作ることを放棄しなければならない．二人がそのことを認識するには，$|S|$ を見積もればよい．この場合，その値はいつも $\sqrt{2}$ 以下になる．これを導くのに，各対の密度演算子を次のように書く．

$$\rho = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b)|\theta_a\rangle\langle\theta_a| \otimes |\theta_b\rangle\langle\theta_b| d\theta_a d\theta_b \tag{2.15}$$

式 (2.13) の相関係数を書き直すと

$$\begin{aligned} S = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b) d\theta_a d\theta_b \quad & \{\cos[2(\phi_1^a - \theta_a)]\cos[2(\phi_3^b - \theta_b)] \\ & + \cos[2(\phi_1^a - \theta_a)]\cos[2(\phi_2^b - \theta_b)] \\ & + \cos[2(\phi_2^a - \theta_a)]\cos[2(\phi_3^b - \theta_b)] \\ & - \cos[2(\phi_2^a - \theta_a)]\cos[2(\phi_2^b - \theta_b)] \end{aligned} \tag{2.16}$$

となり，さらに，

$$S = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b) d\theta_a d\theta_b \sqrt{2}\cos[2(\theta_a - \theta_b)] \tag{2.17}$$

となるので，確率分布 $p(\theta_a, \theta_b)$ に従って状態を準備する場合は常に

$$-\sqrt{2} \le S \le \sqrt{2} \tag{2.18}$$

となる．

もちろん，イブが対になる各粒子の量子状態を完全に制御することはあきらめて，少なくとも一部の対をエンタングルさせるということもあり得る．

もし，すべての対を完全にエンタングルした 1 重項状態に準備してしまったら，イブはアリスとボブのデータを制御できないし，知ることもできないので，二人は容易に秘密鍵を構築できる．実際には，アリスとボブが $|S| = 2\sqrt{2}$ という結果を得ることはあり得ないだろうから，このようなケースは非現実的である．しかしながら，イブが部分的にエンタングルした対を準備した場合でも，量子秘匿性増幅（quantum privacy amplification; 以下 QPA）のアルゴリズム [47] が使えれば，アリスとボブは，完全な秘匿性をもつ鍵を構築できる．部分的にエンタングルした対で，$\sqrt{2} \leq |S| \leq 2\sqrt{2}$ となる場合が最も重要であり，実施可能な鍵分配方式ができたと主張するには，この場合について鍵が構築できることを証明する必要がある．技術的な詳細は省き，ここでは QPA の主要なアイデアのみを紹介する．文献 [47] や 8.4 節に詳しい説明がある．

まず，2 粒子が全体として純粋状態にあるときには，第 3 の物理系とエンタングルしていることはありえないという点に着目しよう．したがって，EPR 対を純粋状態にするような手続きは，いつでも同時にこの対と他の系との間のエンタングルメントを解消してしまうはずである．QPA の方式は，基本的に量子アルゴリズムを繰り返し適用するもので，完全な正確さで実行されれば，混合状態にある複数の EPR 対から出発して，一部の対を捨てる一方，残りの対の状態を 1 重項の純粋状態に収束させる．もし，(現実にはいつでもそうであるように）アルゴリズムが不完全に実行された場合は，繰り返しの各段階の後の対の密度演算子は 1 重項状態には収束せず，それに近い状態に収束する．しかし，その場合でも，盗聴者との間のエンタングルメントの大きさは減少し続けるので，任意の小さい値までもっていくことができる．QPA は，アリスとボブが離れていても，それぞれの場所でのユニタリ変換と測定，および公開チャンネルを通じた測定結果の交換を繰り返すことで実行可能であり，現在開発が進んでいる技術（[48] 参照）によって実現可能であろう．

QPA の手続きの本質的な部分は,「エンタングルメント精製 (entanglement purification)」法 [49] である（8 章参照）．部分的にエンタングルした 2 準位粒子はいつでも精製可能であることが最近示されている [50]．したがって，密度演算子が，直積の状態の混合，すなわち式 (2.15) のように書かれない限りは，アリスとボブはイブに勝てるのである！

2.5　量子盗聴

QPA の手続きには，今日まだ十分に実現可能とは言えないような技術が必要である．そこで，実験の実現性がもっと高いような技術について議論しよう．このことが重要なのは，現行の技術で鍵分配のプロトタイプを組み上げたいからであり，また，それが本当に秘匿性をもつのはどのような条件下なのかを明らかにする必要からである．以下の議論は一般的なものであり，単一粒子による鍵分配にも，エンタングルメントに基づくものにも当てはまる．ただ単に教育的な理由から，アリスがボブに光子を送信する単一粒子方式を仮定して説明している．

2.5.1　エラー訂正

アリスとボブは，まったく同一のビット列を手にすることが不可欠であるから，選別済み鍵の中の食い違いを訂正しなければならない．エラー訂正 (reconciliation または error correction) と呼ばれるこの段階では，公開チャンネルを利用してもよいが，訂正済みの鍵についてはできるだけ少ない情報しかイブに伝わらないようにするべきである（あるいは，公開通信のうちの重要な部分を前もって共有しておいた秘密鍵を用いて暗号化することにした場合には，使う秘密鍵のビット数をできるだけ小さくするべきである）．アリスとボブがデータを訂正するために公開で通信しなければならないビット数の最小値 r は，Shannon の符号化定理 [32] により与えられる．各ビットがそれぞれ独立に，エラー確率 ϵ で間違って伝送される場合を考えると，この定理によれば，n を選別済み鍵の長さとして

$$r = n(-\epsilon \log_2 \epsilon - (1-\epsilon)\log_2(1-\epsilon)) \tag{2.19}$$

となる．

Shannon の定理は構成的な証明がない．すなわち，r ビットしか秘密のデータの情報を公開しないような訂正方式が存在することはわかるのだが，具体的な手続きは定理からはわからない．よく用いられる線形エラー訂正符号は，この点ではかなり非効率である．しかし，Brassard と Salvail によって，Shannon の限界近くまで到達する実用的な双方向型訂正方式が発見されている [51]．この方式は次のようなものである．

アリスとボブは自分のビット列を所定の大きさのブロックに分割する．こ

の大きさは，エラー発生率の関数として最適化しておく．公開チャンネルを通じて，二人は各ブロックのパリティの情報を交換する．二人のパリティが一致すれば，次のブロックに進む．パリティが一致しない場合，そのブロックには奇数個のエラーが存在することがわかる．そのエラーのうちの一つをつきとめるために，ブロックを二つの部分ブロックに分割して，第 1 の部分ブロックのパリティを比較するという操作を繰り返す．すなわち，パリティが一致すれば第 2 の部分ブロックが奇数個のエラーをもつことがわかるし，一致しなければ第 1 の部分ブロックが奇数個のエラーをもつことがわかる．この手続きを，奇数個のエラーがあるとわかった部分ブロックに繰り返していく．

この最初のステップが完了すると，その時点での各ブロックは，偶数個のエラーをもつか，あるいはエラーがないかのいずれかである．アリスとボブは，ここでビットの並ぶ順番を入れ替えて，前よりもブロックの大きさを大きくして同じ操作を繰り返す（この大きさも最適化する）．ただし，ここでまたエラーが一つ訂正されたときに，以前に扱ったブロックの中のエラーの数が奇数個に変わる場合がある．それらも含めた中で，最も小さなブロックを選ぶようにして，前に述べたようにエラー訂正を繰り返す．これを，今までに扱ったすべてのブロック中のエラーの数が偶数個またはエラー無しになるまで続ける．

同様なステップを続けて，この双方向型エラー訂正方式はある所定のステップ数をもって終了する．このステップ数は，食い違いがすべて解消される確率が最大になり，同時に，秘密のデータの漏洩が最小になるように最適化する．はじめ文献 [42] で使われた訂正方式とは異なり，この訂正方式では選別済み鍵のビットを一つも破棄しない．

2.5.2 秘匿性増幅

この時点で，アリスとボブは，高い確率でまったく同一になっている訂正済み鍵を互いに手にしている．二人はまた，正確なエラー発生率 $\bar{\epsilon}$ を把握しており，これがエラー確率 ϵ の非常によい見積もりを与える．アリスとボブは，すべてのエラーが，盗聴を行った可能性のある人物イブによって引き起こされたと仮定する．エラー訂正時に漏洩がある場合には，それも考慮に入れる．そして，訂正済み鍵を τ ビット短くすれば，最終鍵 (final key) についてのイブの情報量が所定の値より小さくなるという値 τ を求める．より

正確に言うと，多くの量子鍵分配方式において，整数 τ が決まったら，アリスはランダムに $(n-\tau)\times n$ の 2 進行列 K（要素が 0 または 1 の行列）を選んで，K をボブに公開で（暗号化せずに）送信する．最終的な秘密鍵は，$\mathbf{k}_{\text{訂正済}}=(k_1,k_2,\ldots,k_n),k_i\in\{0,1\}$ を訂正済み鍵として

$$\mathbf{k}_{\text{最終}}=K\cdot\mathbf{k}_{\text{訂正済}} \pmod 2 \tag{2.20}$$

となる．

秘匿性増幅を実行するのは簡単だが，量子鍵分配方式全体の秘匿性を証明するのは，量子暗号における難しい理論的問題の一つである．そのために，秘匿性の証明は，より強力な攻撃に対して成立するものが徐々に提出されてきた．通常，これらの攻撃は二つの範疇に分けられる．

1. インコヒーレント攻撃（図 2.8）：インコヒーレント攻撃，あるいは個別粒子 (individual particle) 攻撃では，イブが量子プローブ $\mathcal{P}_i$ をエンタングルさせることができるのは，一度に 1 光子だけに限られる．イブは，エンタング

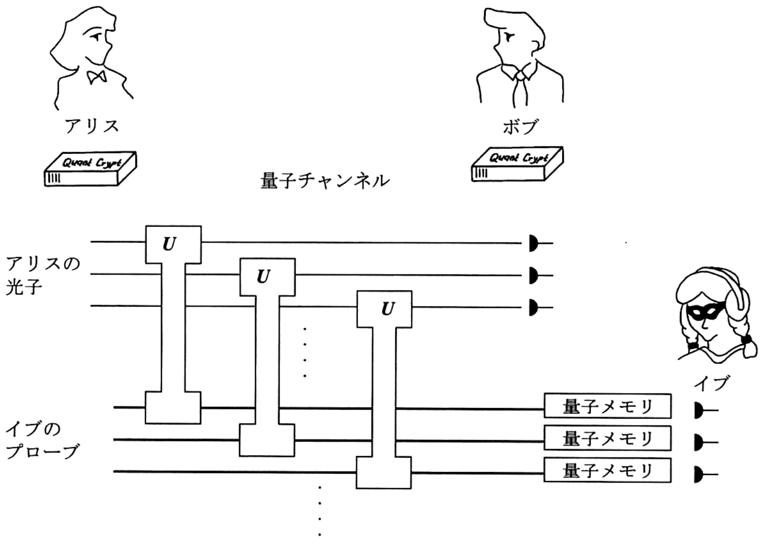


図 2.8　インコヒーレント攻撃：各光子を個別に 2 量子ビットのプローブとエンタングルさせる．プローブは，測定基底が公開されるまで量子メモリに保存する．その後，各プローブを個別に測定する

ルさせた光子がボブによって測定され，アリスとボブの間の公開通信がすべて完了するまで $\mathcal{P}_i$ を保存してもよい．実際，イブのプローブの測定が，ボブの光子の測定の前なのか後なのかは，アリスとボブにとっては知る由もない．したがって，イブにとっての最良の戦略は，アリスとボブが測定基底を公開するまで待った上で，できるだけ多くの情報が取り出せるようにうまい測定を行うことである．ただし，インコヒーレント攻撃では，プローブ $\mathcal{P}_i$ の測定は個別に行われるものに限る．

より詳しく言うと，2.3.1 項で述べたシナリオで，イブのプローブの初期状態を $|E\rangle_i$ と書くと，$\mathcal{P}_i$ をアリスの光子にエンタングルさせる最も一般的なユニタリ変換 $\mathcal{U}$ は，($\oplus$ 基底で) 次のようになる．

$$|E\rangle_i|\updownarrow\rangle \overset{\mathcal{U}}{\mapsto} |E_{00}^{\oplus}\rangle|\updownarrow\rangle + |E_{01}^{\oplus}\rangle|\leftrightarrow\rangle \tag{2.21}$$

$$|E\rangle_i|\leftrightarrow\rangle \overset{\mathcal{U}}{\mapsto} |E_{10}^{\oplus}\rangle|\updownarrow\rangle + |E_{11}^{\oplus}\rangle|\leftrightarrow\rangle \tag{2.22}$$

ここで，$|E_{ij}^{\oplus}\rangle$ は $\mathcal{P}_i$ の規格化されていない状態である．$|E\rangle_i$ は $\{|E_{ij}^{\oplus}\rangle\}_{i,j}$ で張られる空間内にとることができるので，$\mathcal{P}_i$ は 4 次元のヒルベルト空間で記述される，すなわち，各プローブは二つの量子ビットで記述されると仮定してよい．

アリスが $\otimes$ 基底で光子を送った場合，$\mathcal{U}$ の作用は，式 (2.21, 2.22) から線形性を用いて導かれ

$$|E\rangle_i|\swarrow\!\!\!\nearrow\rangle \overset{\mathcal{U}}{\mapsto} |E_{00}^{\otimes}\rangle|\swarrow\!\!\!\nearrow\rangle + |E_{01}^{\otimes}\rangle|\nwarrow\!\!\!\searrow\rangle \tag{2.23}$$

$$|E\rangle_i|\nwarrow\!\!\!\searrow\rangle \overset{\mathcal{U}}{\mapsto} |E_{10}^{\otimes}\rangle|\swarrow\!\!\!\nearrow\rangle + |E_{11}^{\otimes}\rangle|\nwarrow\!\!\!\searrow\rangle \tag{2.24}$$

となる．ここで

$$|E_{00}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle + |E_{10}^{\oplus}\rangle + |E_{01}^{\oplus}\rangle + |E_{11}^{\oplus}\rangle}{2} \tag{2.25}$$

$$|E_{01}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle + |E_{10}^{\oplus}\rangle - |E_{01}^{\oplus}\rangle - |E_{11}^{\oplus}\rangle}{2} \tag{2.26}$$

$$|E_{10}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle - |E_{10}^{\oplus}\rangle + |E_{01}^{\oplus}\rangle - |E_{11}^{\oplus}\rangle}{2} \tag{2.27}$$

$$|E_{11}^{\otimes}\rangle = \frac{|E_{00}^{\oplus}\rangle - |E_{10}^{\oplus}\rangle - |E_{01}^{\oplus}\rangle + |E_{11}^{\oplus}\rangle}{2} \tag{2.28}$$

である．

イブは $\mathcal{U}$ を次のように選ぶ．

1. 盗聴は控えめである．すなわち，たとえばアリスが $|\leftrightarrow\rangle$ を送ったのにボブが $|\updownarrow\rangle$ を観測する確率を，エラーの許容発生率以下に留める．この条件は，ノルム $\langle E_{ij}^{\oplus}|E_{ij}^{\oplus}\rangle$ と $\langle E_{ij}^{\otimes}|E_{ij}^{\otimes}\rangle$，$i \neq j$ が小さいことと等価である（これらの確率は，通常，擾乱 (disturbances) と呼ばれる）．
2. 盗聴は効率的である．すなわち，イブは使用された基底を知り（公開チャンネルを通じてわかる），それに応じた測定をプローブに施すことで，正しいビット値を推定できる確率を最大化する．たとえば，i 番めの光子が $\oplus$ 基底で送られたことをイブが知ったとしよう．もしアリスの対応するビット値が 0 なら，イブのプローブ $\mathcal{P}_i$ は次のような混合状態にある．

$$\rho_0 = \mathrm{Tr}_{\text{光子}}[(\mathcal{U}|E\rangle_i|\updownarrow\rangle)(\mathcal{U}|E\rangle_i|\updownarrow\rangle)^\dagger] \tag{2.29}$$

$$= |E_{00}^{\oplus}\rangle\langle E_{00}^{\oplus}| + |E_{01}^{\oplus}\rangle\langle E_{01}^{\oplus}| \tag{2.30}$$

同様に，もしアリスが光子を $|\leftrightarrow\rangle$ 状態で送った（ビット値 1 に対応）なら，イブのプローブは次のような混合状態にあるはずである．

$$\rho_1 = \mathrm{Tr}_{\text{光子}}[(\mathcal{U}|E\rangle_i|\leftrightarrow\rangle)(\mathcal{U}|E\rangle_i|\leftrightarrow\rangle)^\dagger] \tag{2.31}$$

$$= |E_{10}^{\oplus}\rangle\langle E_{10}^{\oplus}| + |E_{11}^{\oplus}\rangle\langle E_{11}^{\oplus}| \tag{2.32}$$

したがって，イブの目標は，プローブ $\mathcal{P}_i$ の状態が ρ_0 なのか ρ_1 なのかを，できるだけ高い信頼性をもって判定することである．この目標は，$\mathcal{P}_i$ に対しある測定を行うことで達成できることが知られている [52,53]．測定すべき物理量は，その固有ベクトルで指定されるが，この場合，それは $\rho_0 - \rho_1$ の固有ベクトルと一致する．

このエンタングルメントの最適化は，さまざまな単一光子鍵分配方式の場合について，文献 [52]–[56] で詳しく議論されている．これらの結果は，量子チャンネルのエラー確率（あるいは擾乱）と，イブが得た可能性のある最大の情報量とを結びつける．この値（より正確には，それに関連した Renyi 情報量と呼ばれる量）を知ることで，一般秘匿性増幅定理 [57] を用いて，望みの秘匿性を保証する短縮パラメータ τ を計算することができる．もし τ が訂正済み鍵の大きさに比べて十分に小さければ，情報の漏洩は許容範囲内と考えられる．

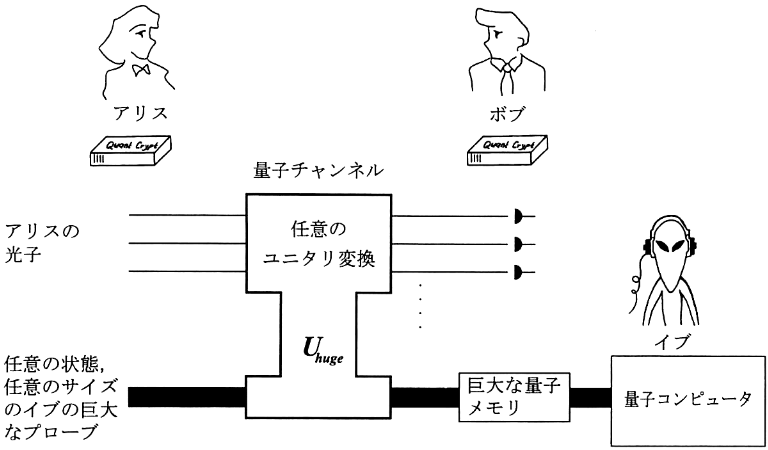


図 **2.9** コヒーレント攻撃：イブは，任意の初期状態にある任意の次元のプローブを用い，それをアリスの送るすべての光子と任意のユニタリな方法でエンタングルさせる．このプローブは，基底が公開されるまで保存される

2. コヒーレント攻撃（図 2.9）：コヒーレント攻撃あるいは連結 (joint) 攻撃では，イブは，任意の状態（混合状態でもそうでなくてもよい）にある任意の次元のプローブを，伝送される光子の列全体と任意のユニタリな方法でエンタングルさせることができる．イブは，この大きなプローブを公開通信が完了するまで保存し，最も一般的な測定を好きに選んで行う．最も一般的な測定のクラスは，正値演算子測度 (POVM: positive operator valued measure) として知られており，詳細は文献 [58] などを参照されたい．

一括攻撃 (collective attack) は（図 2.10），コヒーレント攻撃のクラスの一部分であり，この攻撃では，アリスの光子 i を別々のプローブ $\mathcal{P}_i$ に個別にエンタングルさせる．したがって，イブのプローブの状態はインコヒーレント攻撃のときと同じである．しかし，公開通信が完了した後，イブはプローブ全体を単一の大きな量子系と考えて，それに対して任意の POVM を実行してよい．一括攻撃では，この POVM を施す前は，それぞれのプローブはエンタングルしておらず，互いに独立であることに注意しよう．コヒーレント攻撃に対する秘匿性の主張を証明するのは難しい．これまでのところ，双方向型エラー訂正ではなくて，線形エラー訂正符号を用いる方式のみが考察されて

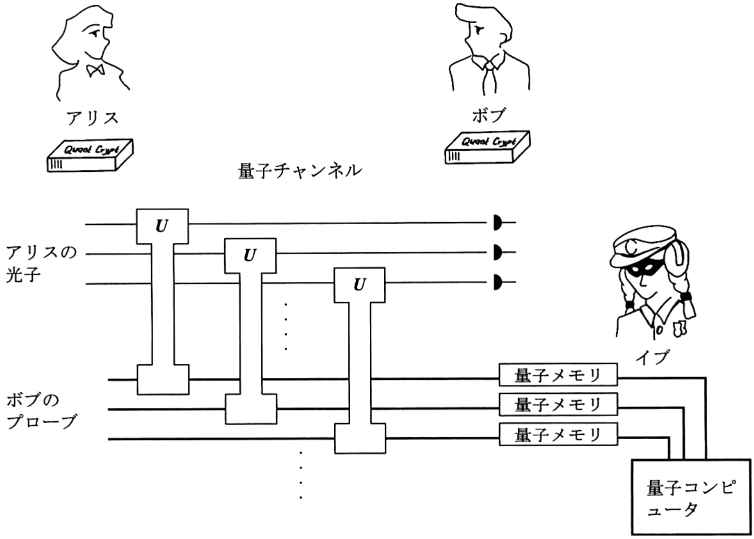


図 2.10　一括攻撃：インコヒーレント攻撃と似ているが，ここではイブは，すべてのプローブを単一の量子系と見て，全体に対して一般化された測定をすることが許される

いる．そのような方式の一括攻撃に対する秘匿性の証明は文献 [59] に，一般のコヒーレント攻撃に対しては文献 [60] にある．

認証：前に述べたように，中間一致攻撃を防ぐためにアリスとボブは通信内容を認証しなければならない．また，二人は新しい秘密鍵を実際に構築できたことを確認しなければならない．幸い，これらの目的を任意の高確率で達成する古典的な暗号技術が存在する．ここでは，認証アルゴリズムの簡明な説明を行い，さらなる詳細は文献 [61] に譲る．認証についての一般的な議論は文献 [30] にある．

仮定として，アリスとボブは秘密の 2 進数の列である認証鍵 $\mathbf{A}$ を共有しているとする．この鍵は，量子鍵分配によって新たに作られる秘密鍵よりは短いけれども，認証のために使うのに十分な長さがあると仮定する．

安全度のパラメータとして，整数 t を選ぶ．アリスがボブに対してデータ $\mathbf{M_0}$ を認証したいとしよう．2 進数の列 $\mathbf{M_0}$ は，たとえば，二人の公開通信のうちあらかじめ決めておいた部分である．長さ m の列 $\mathbf{M_0}$ を，$s = t + \log_2 \log_2 m$

として長さ $2s$ のブロック P_i に分割する（最後のブロックは必要に応じてゼロで埋める）．アリスとボブは，$\mathbf{A}$ の最初の $2s$ ビットを採って数 a とする．$\mathbf{A}$ の続く $2s$ ビットを数 b とする．これら $4s$ ビットは $\mathbf{A}$ から破棄する．そして，二人は，各ブロック P_i について

$$p_i' = ap_i + b \pmod{2^s} \tag{2.33}$$

を計算する．ここで p_i は，2 進数列 P_i によって表現される数である．

結果として得られる数 p_i' を，長さ s のビット列に変換し，つなげて $\mathbf{M_1}$ を構成する．同じ操作を，$\mathbf{M_r}$ の長さが s になるまで（s は一定のままで）r 回繰り返す．$\mathbf{M_r}$ の低位 t ビットがタグ T となる．$\mathbf{A}$ の使用した部分は捨ててしまい，二度と再利用はしない．

最後に，タグ T はボブに送信され，ボブは同じ計算をして結果を比較することで，$\mathbf{M_0}$ が本物かどうかをチェックする．

量子鍵分配方式における認証は，次のように行われる．アリスは，公開通信のうちあらかじめ決めておいた部分を認証する．ボブも，別のあらかじめ決めておいた部分を同じように認証する．この認証が成功すれば，量子鍵分配はうまくいったと考えられ，新しい秘密鍵の小部分を，次回の鍵分配の際の認証鍵として使用できる．このように，アリスとボブは，別の認証鍵を手に入れるために再び会う必要はない．イブが中間一致攻撃をしたと仮定しよう．イブはアリスとある秘密鍵を共有し，ボブとはまた別の秘密鍵を共有する．すべての手続きの間，イブはアリスに対してボブのふりをしていたので，イブはアリスが認証したデータ $\mathbf{M_0}$ を知っている．しかし，T を受け取り，なおかつ $\mathbf{M_0}$ を知っていても，認証鍵をイブが正しく推定する確率は無視できるほど小さいことを示すことができる．したがって，イブは認証テストをくぐり抜けることができない．

2.6 実験による実現

最初の原理実証実験が，IBM－モントリオールのグループ [42]（偏光光子の自由空間伝送による鍵分配）と，オックスフォード DERA のグループ [44]（エンタングルした光子，光ファイバ伝送，位相符号化）により成されたあと，量子暗号の開発は，二つの異なる方向へと続いている．すなわち，一方

では伝送距離，鍵生成レート，量子ビットエラー率 (QBER) についてシステムを最適化することを目指し，同時に他方では，システムをより安定に，また，量子力学や光路のアラインメント調整よりも安全な通信に興味がある将来のエンドユーザにとって，より使いやすくなるようにすべく努力が重ねられている．これまでの節で述べてきたように，さまざまな実装の仕方の背後にある一般的なアイデアは，EPR に基づくシステムを除いてはどれも似ていて，主な違いは変調の種類や解析法である．この節では，量子暗号が現在の技術レベルに至る上で鍵となった発展をいくつか紹介する．

アリスとボブの送信装置と受信装置の信頼性を最大限に高めるのと同時に，重要なのは伝送距離を延ばすことである．一般に，方法は二つある．一つは，アリスとボブの間が直線の光路で結ばれるようにして，テレスコープを用いて光を自由空間で伝送する方法で，もう一つは，光ファイバで光をガイドして 2 点間を結ぶ方法である．伝送方法の選択によって，使う波長は多少なりとも決まってくる．光ファイバは，テレコムウィンドウとも呼ばれる 1300 nm 帯 (0.35 dB/km) と 1550 nm 帯 (0.2 dB/km) で非常に吸収が小さい．しかし，この領域では，必要となる単一光子検出器の開発がそれほどよくは進んでいない [62]．低軌道衛星による自由空間暗号は，どんな距離でも結べるであろうし，地上での最初のテストによれば，そのような量子暗号伝送は少なくとも低いビットレートなら原理的に可能である．

2.6.1　偏光符号化

最初の量子暗号装置では，鍵分配のために数種類の偏光状態が用いられた．標準的な 1 m の光学定盤上で，アリスはまず簡単な発光ダイオード (LED) で弱い光パルスを作り，コリメートして干渉フィルタ (550 ± 20 nm) と偏光フィルタに通す．二つのポッケルスセルにより，アリスは四つの偏光方向（ここでは水平，垂直，左回りおよび右回り円偏光）のうちの一つを選べる．ポッケルスセルは，ある種の結晶では印可電圧に応じて複屈折性が変化するのを利用している．偏光を，たとえば水平から垂直にするときのように 90° 回転させるには，通常 2〜4 kV のオーダのかなり高い電圧が必要である（このことが，実際の応用上でのスイッチングレートを制限する）．32 cm の量子チャンネルの出口で，ボブは，彼のポッケルスセルによって基底を決めて，ウォラストンプリズムを通して光電子増倍管で光子を検出することにより偏光を

分析する．

著者も認めているように，このシステムは，ポッケルスセルの切り替わりの雑音を聞くことで盗聴者に破られてしまう余地があるが，この最初の実演となった実験はすでに量子暗号の多くの魅力的な特性を備えている．本当に初期の段階でもう，量子暗号の実験がいかにシンプルであるかが示されたのだ．これは，量子通信のエンドユーザにとっての利便性を高め，彼らに受け入れられるために必要なことである．さらに，エラー発生率はたった ~ 4.4% に抑えられ，85 秒間にエラー訂正後で 219 ビットの秘密鍵が分配された．

アリスとボブの間の距離を延ばすため，Muller らの実験 [43] では，1 km のファイバ伝送路が用いられた．しかし，ファイバによる偏光符号化システムはいくつかの欠点を克服しなければならない．ボブの装置は，アリスから送られる偏光に合った方向に常にアラインメント調整されていることが必要なのだが，光の偏光はファイバケーブルを通ると変化してしまう．光路の形状によって，トポロジカルな効果がファイバのボブ側の出口での偏光に影響を及ぼす [63]．さらに，応力によって発生する複屈折性のために，偏光の揺らぎと，偏光－モード分散による偏光の減衰が起こる．このため，十分に長いコヒーレンス時間を得るための単一モードレーザや，アリスとボブの間での偏光の能動安定化が必要となる．最後に，送受信装置のさまざまな光学部品は，偏光依存性を最小限に抑えるように注意深く選ぶ必要がある．

より最近になって，偏光符号化装置の安定度が高いという点を活かした自由空間での伝送システムが登場している．大気は本来複屈折性がないので，アリスとボブの装置の相対的なアラインメントの揺らぎを心配する必要がない．屋外の光路での量子暗号 [64] で直面する主な問題は，乱流媒質中での光の伝送と，大きな背景雑音のもとでの単一光子検出である．狭いバンド幅，スペーシャルフィルタ，そしてナノ秒の時間合わせを併用すれば，まずまずのエラー発生率で鍵生成が可能である．ロスアラモスでの最近の実験では，自由空間での光路長 950 m 以上で 14%の結合効率を達成し，約 1.5%のエラー発生率で 50 Hz のビットレート（アリスの送信機のパルスレートは 20 kHz）を得た [65]．この実験は，少なくとも夜間なら，まずまずのビットレートで低軌道衛星による秘密鍵の構築が実現可能であることを示している．

2.6.2　位相符号化

2.3.2 項で指摘したように，偏光での符号化と同じようにして位相による符号化ができる．図 2.6 に示したマッハーツェンダー型が外部からの影響を非常に敏感に受けてしまう点は，Bennett により提案された非平衡マッハーツェンダー型の構成 [45] により解決できる．二つのコヒーレントな成分はわずか数ナノ秒だけの差をつけられて同一のファイバを伝播するので，本質的に温度や応力に起因するゆらぎは生じない．ボブ側の非平衡干渉計の光路長差は，アリス側のものと同じでなければならず，波長より短いスケールで安定に保つ必要がある．しかし，そのためには単に干渉計の温度安定化をそれぞれの場所で注意深く行うだけでよい．

位相変調器は二つのテレコム波長帯で製品化されており，標準的な位相符号化法は，おそらくファイバで実装する際の最善の選択肢だろう．しかしながら，そのような方式でも，やはり偏光の問題から厳しいアラインメント条件が生じる．当然ながら，二つの非平衡マッハーツェンダー干渉計では，ボブの出力のビームスプリッタで干渉する成分が同じ偏光をもつように，偏光を制御しなければならない．最初にアリスとボブの装置を調整してしまえば，これは安定に保たれ，以後は問題にはならないはずである．より困った問題は，位相変調器を構成する電気光学結晶が，二つの偏光成分のうちの一方だけしか光をまともに通さないということから生じる．ボブの出力での強度揺らぎを抑えるためには，よく定まった一つの偏光成分だけしか変調器を通せない．このために，またもや伝送時の偏光の制御が必要となる．

Townsent らの実験 [66] では，レーザから来るパルス (1.3 μm，80 ps) をまずアリスの非平衡マッハーツェンダー干渉計の二つの経路に振り分ける．一方の腕では，位相変調器により，BB84 方式に従い 4 種類の位相シフトのうちの一つが印可される．もう一方の腕では，偏光を回転し，アリスの出力のビームスプリッタで二つの成分の偏光が直交するようにする．ボブの入力のビームスプリッタは，偏光ビームスプリッタに置き換えて，正しい偏光成分をもつほうがボブの位相変調器のある腕に向かうようにする．伝送路の出口に置く偏光制御器は，これら二つの偏光方向と，ボブの入力の偏光ビームスプリッタの軸が一致するように調整する．このような方式では，偏光の安定化が再び必要になってしまうが，小さなずれならば最終的な強度の揺らぎは

無視できる程度なので，安定化の要求レベルはそれほど厳しくない．1 MHz ものパルスレートで，4%以下のエラー発生率が達成されている．ロスアラモスのグループは，さらに改良を重ね，48 km を超える地下ファイバケーブルでの伝送で，30 kHz のパルスレートで約 1%のエラー発生率を達成した [67].

いわゆる「プラグ＆プレイ」システムでは，ファイバ伝送での偏光のアラインメント調整を継続的に行う必要がない．ベースとなるアイデアは，光パルスをアリスの場所ではなくボブ側で発生し，まずそれをアリスに送り，変調した上で反射してボブに戻すというものである．この方式における反射をファラデーミラーによって行うと，ボブの出力において干渉する成分の偏光は常に揃ってしまう．

ファラデーミラーは，45° のファラデー回転子と垂直入射ミラーから成り，ファイバに入る光と反射して戻る光が直交する．このため，伝送路や干渉計の腕で生じるどんな偏光の変化も効果的にキャンセルしてしまう．

このアイデアを用いて 4 状態の BB84 方式を実装したシステムを図 2.11 に示す [68]．この実験では，伝送路として標準のテレコムファイバケーブルを使用し，アリスとボブは 23 km 離れている．継続的な能動安定化を一切行わずに，1% という低いエラーが達成され，正味の鍵生成レート 210 Hz が得られた．テレコム波長 1300 nm で行われたこれらの実験では，どれもノイズの大半は単一光子検出器（ペルチェ冷却で届く 173 K までしか冷却していない InGaAs/InP アバランシェフォトダイオード）の高いダークカウントレートに起因している．現在のところ，うまく同期をとりゲート検出回路を用いることで雑音レベルを下げているが，検出器がさらに改良されれば，今後の量子暗号の応用にものすごい影響を与えるだろう．

2.6.3 エンタングルメントに基づく量子暗号

エンタングルした粒子の対の非古典的な性質を利用すれば，多くの新しい特色を暗号に活かすことができる（2.4 節参照）．しかし，そのような方式は，程度の高いエンタングルメントを作らなければならないという主な理由のために，現在の技術ではこれまで述べた単一粒子による試みに比べて実現が難しい．アリスとボブの間に不完全なエンタングルメントが配られたとしても，そのエンタングルメントの大きさを改善するには，エンタングルメント精製のような，現在の技術では実現できない技術が必要になる．というわけで，エ

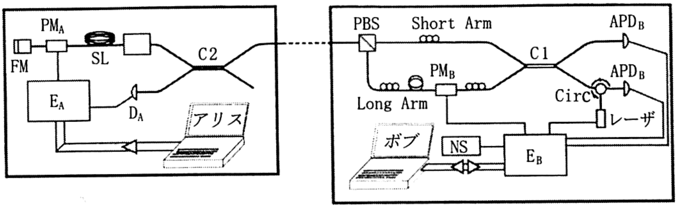


図 2.11　プラグ&プレイ量子暗号の原理：ボブはサーキュレータ (Circ) を通して光パルスを送る．このパルスはカプラー C1 で分割される．最初の半分は短い腕 (Short Arm) を通る．偏光制御器は，このパルスが偏光ビームスプリッタ PBS で完全に透過するように調整する．パルスはアリスに送られ，カプラー C2 で再び分割され，タイミング用の信号を与える．パルスはアリスの装置を通過した後，反射してボブに戻される．ファラデーミラー FM のおかげで，光路における複屈折性は補償され，パルスは直交する偏光になって戻ってくる．続いてこのパルスは PBS で反射され，長い腕 (Long Arm) を通り，ここでボブは変調器 PM で位相シフト ϕ_B を与える．第 2 のパルスは，二つの腕を逆の順番で通過する．アリスはこのパルスに位相シフト ϕ_A を与える．両パルスはまったく同じ光路をたどるので，カプラー C1 に同じ偏光で同時に到達し，干渉が起こる．レーリー後方散乱のために生じる問題を回避するため，アリスのシステムにはストレージライン SL が設けられている

ンタングルメントにおけるノイズがそのままシステムの性能を決めてしまう．そこで，最初の実験 [44] 以来，主な目標はエンタングルした光子対の光源の開発を進めることであった．今日では，パラメトリック下方変換が光子対の光源として使われている．この過程は効率が低いので，十分なビットレートのためには広帯域の光を使用する必要がある．そうなると，光子対を分散のある光ファイバで伝送する際の問題を避けるため，妥協点を見つけなければならない．

多くの試みでは，時間–エネルギーのエンタングルメント（詳細は文献 [69,70]）が用いられている．パラメトリック下方変換過程で光子対を生成すると，二つのマッハーツェンダーあるいはマイケルソン干渉計（ただし非平衡で，各干渉計の光路長差が下方変換のポンプレーザのコヒーレンス長よりも短い場合）の出力の間で非局所的な干渉を起こすことが可能である．干渉

している部分と干渉していない部分とを区別するためには，検出イベントを時間によって選別する必要がある．単一光子検出器の最小時間分解能がおよそ 300 ps なので，対応する光路長差約 30 cm が必要となる．ジュネーブで行われた EPR-Bell 問題についての実験は，エンタングルした対を標準のテレコム線で物理的距離が 10 km 離れた二つの検出器まで伝送（光源と検出器を結ぶ 2 本の光ファイバの実際の長さは 8km と 9km）しても，まだ程度の高いエンタングルメントが観測できることを示した [71].

偏光のエンタングルメントも，やはりパラメトリック下方変換過程（タイプ II，文献 [16]）によって作ることができる．最近の実験では，観測者が独立な場合でもベルの不等式の破れが観測された [72]．この実験では，二人の観測者，アリスとボブは，約 400 m 離れていた（二人を結ぶ光ファイバは 1km）．ただし，ここで偏光分析のランダムな方向を決めるところから光子の検出に至るまでのすべての測定に要した時間 ($\sim$ 80 ns) は，二人の間で情報を伝えるのに要する時間 ($\sim$ 1300 ns) よりもはるかに短い．この実験用に開発された，速い電気光学変調システムと検出回路は，真の単一光子状態により秘匿通信を保証する量子暗号と，ベルの不等式の破れによる量子暗号のどちらにもそのまま用いることができる．

2.7　おわりに

多様な展開を見せる量子暗号の研究は非常に活発なものになってきており，この分野の包括的なレビューを行ってもすぐに現状に追い抜かれてしまうだろう．そこで，ここでは，分野に入っていく上でのよい出発点として役立つことを願って，非常に基本的な知識のみを提供することにした．基本的なメッセージはこうである：今日の量子暗号は，従来の暗号化の手法と並ぶ実行可能な選択肢であり，そう遠くない将来には，機密の通信は数論ではなくて量子力学に頼らなければならなくなるかもしれない．

ここで述べたことは，現在の動向のほんの表面をかすっているに過ぎないことに注意してほしい．2 者間での秘匿計算，量子認証の詳細，盗聴技術と秘匿性基準の細かい分析，鍵分配を行う別種の技法（たとえば，直交した状態を二つの部分に分けて伝送する仕組みに基づく Vaidman と Goldenberg の方法）などのトピックは省略した．これらのトピックあるいは関連したトピックについては，

ロスアラモス国立研究所の e-print archive (http://xxx.lanl.gov/archive/quant-ph)，あるいは，http://www/qubit/org をはじめとする他の WWW サーバに，多数の興味深い論文が置かれている．

第3章

量子稠密符号化と量子テレポーテーション

3.1　はじめに

(*D. Bouwmeester, H. Weinfurter, A. Zeilinger*)

2章ではどのようにして量子エンタングルメントが暗号鍵分配に利用されるかを説明した．本章ではエンタングルメントを用いることで，他にどのようなタイプの量子通信が可能になるのかを示すことにしよう．まず3.2節では量子稠密符号化（Quantum Dense Coding）を取り上げる．これは個々の粒子は1ビットの情報しか担えなくても，二つの粒子がエンタングルしている場合には，片方の粒子のみを操作して送信するだけで2ビット分の情報が伝えられるというものである[73]．続く3.3節では量子テレポーテーションを概観する．量子テレポーテーションとは，ある量子系の上に準備された状態をエンタングルメントを介して離れた場所にある別の量子系の上へと移すことであり，Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters[74]によりはじめて提唱された．

これらの新しいタイプの量子通信の実証実験は，主として量子光学の方法を用いることにより行われてきた．その場合に不可欠なのは，エンタングルした複数光子の系の生成と，いわゆるベル状態測定の光学的な実現である．

そこでまず，3.4 節および 3.5 節ではそれぞれ前者および後者について解説しよう．次に 3.6 節では量子稠密符号化の実証実験 [75] を紹介する．続く 3.7，3.8，3.9 の各節では，量子テレポーテーションに関するいくつかの実験について考察しよう．まず 3.7 節では，インスブルック大学で行われた実験 [76] を説明する．この実験では 2 光子系の偏光エンタングルメントを介して単一光子の偏光状態に対する量子テレポーテーションを行っている．次に 3.8 節では，Popescu[77] により提案されローマ大学において行われた実験 [78] について説明する．この実験では，運動量についてエンタングルした 2 光子の対を準備し，その一方の光子の上に準備された偏光状態を量子テレポーテーションによって離れた場所にある他方の光子上へと転送している．3.9 節では連続量の量子テレポーテーションを取り上げる．この方法は Vaidman[79] により最初に提唱され，Braunstein と Kimble による発展を経て，その後カリフォルニア工科大学において実証された [81]．これらの異なる実現方法にはそれぞれ長所と短所がある [82]-[84]．

量子テレポーテーションの対象となる量子状態が，他の量子系とエンタングルしている量子系の上に準備されている場合には，直接の相互作用を伴わないにもかかわらず，量子テレポーテーションの結果として，二つの離れた系の間にエンタングルメントが生じる．3.10 節と 3.11 節では，このようなエンタングルメント・スワッピング (Entanglement Swapping) と呼ばれる過程について説明し，そのいくつかの利用方法を述べる [85]-[87].

3.2　量子稠密符号化の基本手順

Bennett と Wiesner による量子稠密符号化の提案 [73] では，それぞれ直交する二つの量子状態 $|0\rangle$ と $1\rangle$ とを取りうる二つの量子ビット (qubit) 粒子間にあるエンタングルメントを用いている．古典物理学の立場では量子ビット粒子を二つ用いれば 00，01，10，11 の四つの組み合わせが可能であり，それぞれの粒子を独立に操作することで，全体としては 2 ビットの情報を符号化できる．

さらに量子物理学の立場では，これらの四つの組み合わせに関する量子力学的な重ね合わせ方の違いを利用して，2 ビット情報を符号化することが可能になる．このように，複数の粒子についての直積状態をさらに量子力学的

に重ね合せることで得られる量子状態のことを，1.4 節で説明したようにエンタングル状態と呼んでいる．二つの量子ビットからなる系のエンタングル状態を記述するときには，最大にエンタングルした四つのベル状態を直交基底として選ぶのが便利である．

$$|\Psi^+\rangle_{12} = (|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)/\sqrt{2} \tag{3.1}$$

$$|\Psi^-\rangle_{12} = (|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)/\sqrt{2} \tag{3.2}$$

$$|\Phi^+\rangle_{12} = (|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)/\sqrt{2} \tag{3.3}$$

$$|\Phi^-\rangle_{12} = (|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2)/\sqrt{2} \tag{3.4}$$

ここで式中の添え字 1 と 2 はそれぞれ粒子 1，2 を表す．これらの四つのベル状態を用いて二つの量子ビットからなる系に 2 ビットの情報を符号化できる．しかしながら古典的な場合とは異なり，片方の量子ビットを操作するだけで 2 ビットの情報が符号化できてしまうのである．

その基本手順を以下に説明しよう．アリスとボブはベル状態 $|\Psi^+\rangle_{12}$(3.1) に準備された 2 粒子系の粒子 1 と 2 をそれぞれ手元に保管しているとする．次にボブは，以下に述べる 4 通りのユニタリ変換の中からどれか一つを選んで粒子 2 に作用させる．ここで 4 通りのユニタリ変換とは

1. 恒等変換（状態 $|\Psi^+\rangle_{12}$ にいかなる変更ももたらさない）
2. 粒子 2 の状態を反転 ($|0\rangle_2 \to |1\rangle_2, |1\rangle_2 \to |0\rangle_2$:その結果 $|\Psi^-\rangle_{12} \to |\Phi^+\rangle_{12}$ となる)
3. 粒子 2 の状態に依存した位相シフト ($|0\rangle_2$ なら 0 シフト，$|1\rangle_2$ ならシフト：その結果 $|\Psi^+\rangle_{12} \to |\Psi^-\rangle_{12}$ となる)
4. 2 と 3 を一緒に行う （その結果 $|\Psi^+\rangle_{12} \to |\Phi^-\rangle_{12}$ となる）

である．

最初のベル状態 $|\Psi^+\rangle_{12}$ はこれらの四つの操作のそれぞれによって，それぞれ異なるベル状態へと変換されるので，ボブから粒子 2 を受け取った後でアリスが 2 粒子系のベル状態を判定すれば，粒子 2 それ自体は 2 状態粒子であるにもかかわらず，4 通りの識別可能なメッセージすなわち 2 ビットの情報が，ボブからアリスへと伝えられることになる．このようにして，通信路の容量は古典的に可能な最大値 1 ビットから 2 ビットへと増強されるのである[1]．

[1]確かにボブがアクセス可能な光子の通信路の容量は 2 ビットまで増強されてはいるが，アリスのもとに

3.3　量子テレポーテーションの基本手順

本節では，Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters によって提唱された量子テレポーテーションの基本概念について図 3.1 を参照しながら説明しよう．

アリスは未知の量子ビット状態 $|\Psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$ にある粒子 1 をもっている．ここで $|0\rangle, |1\rangle$ は直交する二つの状態であり，複素振幅 α,β は $|\alpha|^2 + |\beta|^2 = 1$ を満たす．アリスは粒子 1 の量子ビットの状態をボブに伝え

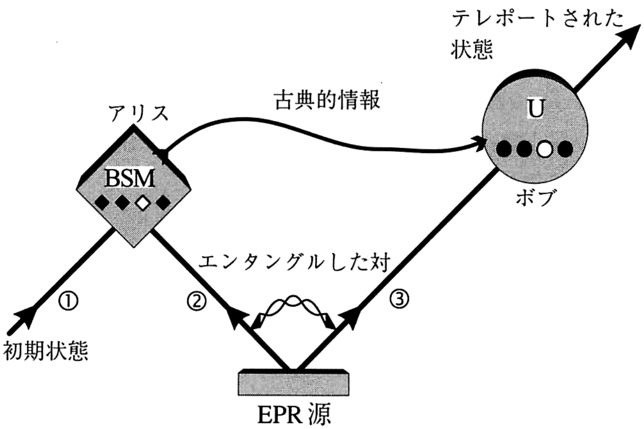


図 3.1　量子テレポーテーションの基本原理：アリスは粒子 1 をもっており，その初期状態はボブに転送したい量子状態に準備されている．そのほかに，アリスとボブは，Einstein-Podolsky-Rosen (EPR) 粒子源によって発生したエンタングルした粒子 2 と粒子 3 をそれぞれ分け合っている．次にアリスは，粒子 1 と粒子 2 の対に対してベル状態測定を行って，対の状態をエンタングル状態に射影する．アリスは測定結果を古典情報としてボブに伝え，ボブはそれに基づいて粒子 3 に対して適切なユニタリ変換を施す．その結果，粒子 1 の上に準備された初期状態は粒子 3 の上に移動する．量子ビットに対する量子テレポーテーションの場合には，アリスは完全直交基底系を成している四つのベル状態のどれか一つの状態への射影測定を行う．2 ビットの情報に相当する測定結果をボブに知らせれば，ボブは量子ビットの初期状態を再生することができる

あらかじめ 0 ビットの情報を含んだもう一つの光子（粒子 1）が送られていなければならないことに注意しよう．結局全体の容量が 2 ビットを越えることはない．

たいのだが，粒子 1 それ自体を直接ボブに送ることはできないものとしよう．もし仮にアリスが α と β の値を測定によって決めることができて，その結果をボブに伝えることが可能ならば，ボブはその量子ビットの状態を容易に再構成できるだろう．しかしながら量子力学の射影定理によれば，アリスによるいかなる測定も粒子 1 の量子状態を破壊してしまうため，再構成に不可欠な α と β についての情報を共に得ることは原理的に不可能である．よってこの自明な方法は使えない．それでは，どうすればボブに粒子 1 の量子ビット状態を伝えることができるだろうか．この問題は，粒子 2 と粒子 3 からなるエンタングル状態（EPR 対）を補助的に利用することで見事に解決される．ここでそれぞれアリスとボブの手元にある粒子 2 と粒子 3 は，式 (3.5) で表されるベル状態 $|\Psi^-\rangle_{23}$ を形成している．

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3) \tag{3.5}$$

エンタングル状態として $|\Psi^-\rangle_{23}$ を採用するのには理由がある．それは測定によって粒子 2 の状態が $|0\rangle$ と $|1\rangle$ の規格化された線形結合状態に射影されたとき，粒子 3 の状態は粒子 2 の状態とは直交した状態に射影されるからである．式 (3.5) の右辺の二つの項が逆位相の関係にあるために，偏光測定における基底のとり方とは無関係に，粒子 2 と粒子 3 の量子状態は常に直交することに注意しよう．

たとえ粒子 1 と粒子 2 がエンタングルしていなくても，これらの粒子系の偏光についての直積状態は式 (3.1)～(3.4) で与えられる四つのベル状態基底によって展開できる．そこでまず，三つの粒子 1，2，3 からなる全系の量子状態 $|\Psi\rangle_{123}$ を以下のように表してみよう．

$$\begin{aligned}|\Psi\rangle_{123} = |\Psi\rangle_1 \otimes |\Psi\rangle_{23} = \frac{1}{2}\ \big[\ &|\Psi^-\rangle_{12}\,(-\alpha|0\rangle_3 - \beta|1\rangle_3)\\ +\ &|\Psi^+\rangle_{12}\,(-\alpha|0\rangle_3 + \beta|1\rangle_3)\\ +\ &|\Phi^-\rangle_{12}\,(\alpha|1\rangle_3 + \beta|0\rangle_3)\\ +\ &|\Phi^+\rangle_{12}\,(\alpha|1\rangle_3 - \beta|0\rangle_3)\ \big]\end{aligned} \tag{3.6}$$

粒子 1 と粒子 2 に対してアリスはベル状態測定（すなわち，2 粒子の状態を四つのベル状態の中のどれか一つに射影する）を行う．その結果，ボブの手元にある粒子 3 は，粒子 1 の初期状態 $|\Psi\rangle_1$ と直接に相関した状態に見いだ

されることになる．たとえば，アリスの測定結果が $|\Phi^-\rangle_{12}$ であったら，粒子 3 は状態 $\alpha|1\rangle_3 + \beta|0\rangle_3$ に見いだされる．測定の後でアリスがすることは，自分の測定結果を古典通信路によってボブに伝えることだけである．その後で，ボブは粒子 1 の初期状態を再現するために，粒子 3 に対して適切なユニタリ変換 U を施せばよい．このようにして量子テレポーテーションが完了する．

量子テレポーテーションの一連の過程において，複素振幅 α,β の値それ自体は未知のままであることを強調しておこう．ベル状態測定は，転送される量子ビットについてのいかなる情報もアリスにもたらさず，ただ単に量子状態を転送するための一操作であるにすぎない．その上，粒子 1 の初期状態 $|\Psi\rangle_1$ はベル状態測定によって完全に破壊されてしまう．なぜならば，ベル状態測定によって粒子 1 は粒子 2 とエンタングルしてしまうからである．状態 $|\Psi\rangle_1$ は量子テレポーテーションによってボブの側に移されるのと引き替えにアリスの側では完全に消滅してしまうのである．これは量子力学のノークローニング (no-cloning) 定理 [88] の意味するところでもある．粒子 1 の初期状態はアリスのみならず他の何人にとっても未知であり，またベル状態測定が行われた時点で粒子 1 単独の量子状態を定義することはもはや不可能である．Bennett らによって指摘されたように，粒子 1 は粒子 2 とエンタングルすることによって，粒子 1 としての独自の量子状態を失ってしまうのである．この視点をさらに進めると，3.10 節で説明されるエンタングルメント・スワッピングの着想に辿りつく．

量子テレポーテーションや量子稠密符号化およびエンタングルメント・スワッピングを行うためには，エンタングルした粒子の系の準備とベル状態測定が不可欠である．続く二つの節では，これらを実現するための量子光学的な方法について説明しよう．

3.4　エンタングルしている光子系の生成

(N.Gisin, J.G. Rarity, G. Weihs)

エンタングルしている粒子の系を作るにはいろいろな方法がある．これらのうち，共振器中の量子電気力学過程によってエンタングルした原子の系を生成する方法については 5.2.3 項で，またポール電磁トラップによってエンタ

ングルした少数イオンの系を作り出す方法ついては5.2.11項で述べる．5.3節では，単一分子の中に形成された核スピン間のエンタングルメントを核磁気共鳴の方法により制御する方法について解説している．固体電子素子中でのエンタングルメント生成の試みは，今後の発展が期待されるとはいえ制御可能なエンタングルメント粒子系としての実現性はいまだ明らかではない．そこで本節では，良質なエンタングルメント粒子系を生成する方法として，現時点では最も成功している量子光学的な方法によるエンタングルメントの生成について解説することにしよう（エンタングルメント生成の一般論については1.5節を参照せよ）．

量子光学的な方法には大きく分けて二つの方法がある．一つは，複数の単一光子の量子状態の間にエンタングルメントを生成する方法であり，これが本節のテーマである．もう一つは，複数の光波（波数ベクトルが同じでも偏光モードが異なれば異なる光波とみなそう）の直交位相振幅成分（つまり振動電磁場のsin成分とcos成分に対応）の間にエンタングルメントを生成する方法であり，これについては3.9.2項で取り上げる．

3.4.1 パラメトリック下方変換

多くの量子光学実験において，非線形光学過程は重要な役割を果たしている．非線形光学自体は古典電磁気学の一分野であり，ある種の媒質中における強い光波間の非弾性相互作用を取り扱うものである．光波間の非弾性相互作用とは，電気感受率で記述される媒体を介した光波間の相互作用によって，光波の方向や周波数などが変化するということである．このような相互作用の一例として（入射した光波とは別の）新しい光波が励振されることがある．たとえば，媒体の電気感受率を光電場の強度で展開すると，最低次の効果として3光波混合や4光波混合が導かれる．ここで媒体中の電気分局$\mathbf{P}$の独立な成分P_iは

$$P_i = \chi^{(1)}_{ij}\, E_j + \chi^{(2)}_{ijk}\, E_j\, E_k + \chi^{(3)}_{ijkl}\, E_j\, E_k\, E_l + \cdots \tag{3.7}$$

により与えられる．ここでE_iは電場のベクトル成分である．

波長に比べてずっと大きい媒体中における非線形相互作用を観測するためには，媒体全体からの寄与を考慮しなくてはならず，媒体の異なる部分からくる寄与の干渉効果のために関与する複数の光波の波数ベクトルの間にはい

わゆる位相整合条件が課されることになる．

さらに量子電気力学によれば，原子からの光子放出過程と同様に，誘導放出過程だけでなく自然放出過程も生じることが示される．非線形相互作用に基づく光子の自然放出過程は Klyshko[89] によりはじめて理論的に考察され，Burnham と Weinberg により実証された [90]．それらの中でも特に重要なのは 2 次 $(\chi^{(2)})$ の非線形光学効果の一つである自然パラメトリック下方変換である．周波数の ω_p のポンプ光波を入射すると，媒体との非線形相互作用によって周波数 ω_1 と ω_2 の二つの光子が自然に放出される．相互作用におけるエネルギー保存則から

$$\omega_1 + \omega_2 = \omega_{\mathrm{p}} \tag{3.8}$$

が満たされる．さらに位相整合条件

$$\mathbf{k}_1 + \mathbf{k}_2 = \mathbf{k}_{\mathrm{p}} \tag{3.9}$$

が満たされなければならない．ここで位相整合条件を満たしうる波数は，光の周波数や媒体の種類に依存していることに注意しよう．自然放出の効率は $\chi^{(2)}$ の大きさによって支配され，一般には非常に小さい．たとえば，PDP (potassium di-deuterium phosphate) や BBB (β-barium borate) などの高い非線形感受率をもつ厚さ 2，3mm の光学結晶に真空紫外領域の強度 100mW のポンプ光を入射した場合でさえ，毎秒発生する光子の数は 10^{10} 程度にすぎない．その上 $\chi^{(2)}$ 非線形を有する結晶は反転対称性がないものに限られるため，そのような非線形光学媒体の候補は限られてしまう．

可視光領域でのパラメトリック下方変換の位相整合条件には二つのタイプがある．下方変換により生じた光子の偏光状態はタイプ I の位相整合では平行であるが，タイプ II の位相整合では結晶軸の向きによって定まる互いに直交する偏光モードのそれぞれを各々の光子が占めることになる．パラメトリック下方変換では二つの光子は同時に発生している上に，それらの波数ベクトルの関係は位相整合条件の制約を受けている．このような特徴をもつがゆえに，パラメトリック下方変換はエンタングルメントの生成とその測定を行うための有用な手段たりうる．

3.4.2　時間についてのエンタングルメント

パラメトリック下方変換によって生じた光子対はさまざまな特徴的な性質

をもっている．タイプI，タイプIIともに，まず時間についてのエンタングルメントが見いだされる．これは二つの光子が同時に発生していることと，エネルギー保存側が満たされていることからの単なる帰結である．光子対の発生時刻それ自体はポンプ光のコヒーレンス時間幅に相当するだけの不確かさをもつ．一方で，対をなす光子のそれぞれは波長に換算してナノメートル程度の広い周波数帯域幅をもっているため，ポンプ光のそれと比較してはるかに短い100フェムト秒程度のコヒーレンス時間しかもっていない．この種のエンタングルメントの効果はフランソン (Franson) 干渉計（図3.2を参照）によって顕著に見ることができる．図3.2に見るように，二つの光子はそれぞれ左右にある非対称マッハ-ツェンダー干渉計へと導かれる [91]．左右の干渉計の構成は同一であり，異なる二つの光路の伝播時間差がそれぞれの光子のコヒーレンス時間より十分長くなるように作られている．そのため，それぞれの干渉計の出力を計数しても1光子干渉が現れることはない．しかしながら，もし両側の干渉計の出力についての同時計数率を測定すると，干渉の効果——すなわち干渉計の異なる光路の間の位相差を変えていくと同時計数率が振動する——を観測することができる．フランソン干渉計中の2光子の状態は

$$|\Psi\rangle = \frac{1}{2}\Big[|S\rangle_1|S\rangle_2 + e^{i(\phi_1+\phi_2)}|L\rangle_1|L\rangle_2 + e^{i\phi_2}|S\rangle_1|L\rangle_2 + e^{i\phi_1}|L\rangle_1|S\rangle_2\Big] \tag{3.10}$$

によって表される．ここで添え字1と2は，図3.2においてそれぞれ，左と右に向かう光子を表している．式(3.10)の量子状態自体は実は直積状態である．しかし，式(3.10)の右辺の四つの項の中で同時計数をもたらすのはL-Lの項とS-Sの項だけであり，他の項からの寄与は適切な同期ゲート処理により除去することができる．初期の実験ではこの同期ゲート処理を省いていたため干渉の可視度は50%止りであった [91]．現在では高速な同期ゲート処理によって，エンタングル状態の寄与だけを事後選択（ポストセレクション）することにより，干渉の可視度は90%を上回るようになっている [92]．

その後の実験的な改良にもふれておこう．図3.3では，連続光ではなくパルス光をポンプ光として採用し，パルス幅よりも光路長差が長い非対称干渉計を通過させることで2連ポンプパルス光を作り出している [93]．ポンプ光

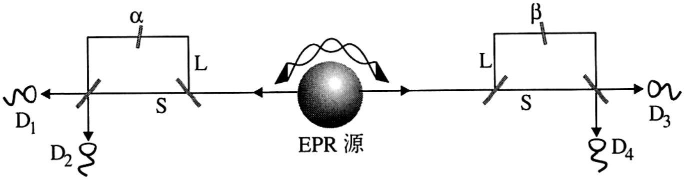


図 **3.2**　時間についてエンタングルしている二つの光子の干渉を調べるために Franson により提唱された干渉計（フランソン干渉計）の概念図：両側にはそれぞれ光路長差のあるマッハーツェンダー干渉計がついており，それぞれの干渉計における位相差は長い経路中におかれた位相シフタによって調整される

中の光子が結晶中で光子対に下方変換される時刻は一意には定まらず，2連パルス中のポンプ光子の状態が重ね合わせ状態 $\alpha|\mathrm{short}\rangle_{\mathrm{pump}}+\beta|\mathrm{long}\rangle_{\mathrm{pump}}$ になっているため，下方変換で生じた光子対の状態は

$$\alpha|\mathrm{short}\rangle_{\mathrm{s}} \otimes |\mathrm{short}\rangle_{\mathrm{i}} + \beta|\mathrm{long}\rangle_{\mathrm{s}} \otimes |\mathrm{long}\rangle_{\mathrm{i}} \tag{3.11}$$

となっている．ここでは（入り口の）非対称干渉計によってコヒーレンスが確保されるので，連続ポンプ光の場合と異なり，ポンプ光波のコヒーレンスはもはや制約ではないことに注意しよう．ポンプ光子が結晶に到着する時刻の拡がりの幅（ポンプ光波のコヒーレンス時間の幅に相当）が $|\mathrm{short}\rangle$ と $|\mathrm{long}\rangle$ に対応する二つの値に置き換えられているのである．したがって，コヒーレンス時間の短い光源（たとえば半導体レーザなど）をポンプ光源として利用することが可能になる．さらに到着時刻を識別することによって $|\mathrm{short}\rangle$ か $|\mathrm{long}\rangle$ かを判別できるし，非対称干渉計における結合比と位相を操作することによって，2量子ビットの量子通信に必要なあらゆるエンタングル状態を作り出すこともできる．

3.4.3　運動量についてのエンタングルメント

平行ではない二つの光子ビームを出力するパラメトリック下方変換を利用すると，運動量についてのエンタングルメントを作り出すことができる．これは二つの光子が異なる波長で異なる方向に放出されるときに位相整合条件による制約を受けることに起因している．図3.4中に描かれたスリットAによって，放出方向について異なる組み合わせをもつ独立な二つの光子対モードにある下方変換光子対が選別される [94]．具体的には，片方の光子の周波

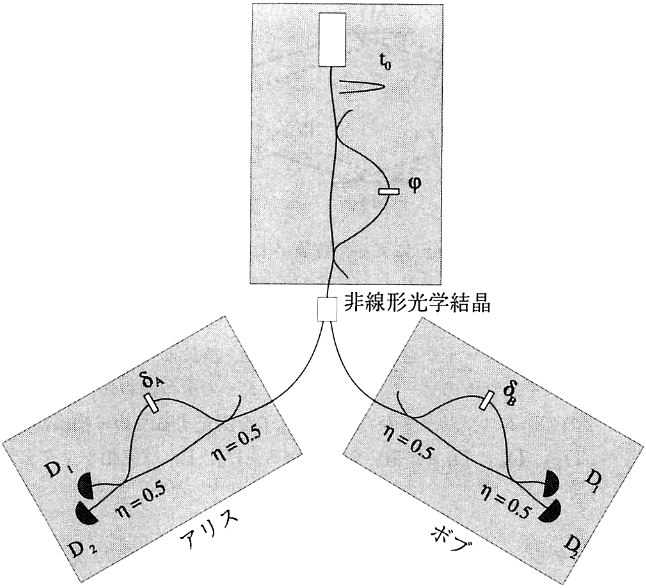


図 3.3 時間についてエンタングルしている光子の対を生成するパルス光源の概念図と，その量子暗号への応用：第 1 の干渉計において，それぞれ短い経路と長い経路を通過したポンプ光子により発生した光子対は，互いに可干渉である．アリスとボブは（出射時刻に対して）三つの異なる遅延時間（長い，短い，中間）のいずれかにおいて二つの光子を検出することになる．そのうち遅延時間が長いまたは短い場合には発生時刻に関して 100%の相関がある．中間の場合は，重ね合わせ状態 $|\mathrm{short}\rangle \pm |\mathrm{long}\rangle$ を基底として選んだことに相当しており，$\varphi + \delta_A + \delta_B = 0$ の条件のもとでは（干渉計の出力に）完全な相関が見られる．この系の特徴は乱数発生器や能動光学部品を必要としないことである

数がポンプ光の周波数の半分 $\omega_p/2$ よりやや高ければ（カラー a）もう片方の光子の周波数は $\omega_p/2$ よりやや低く（カラー b）なるように選別される．こうして光子対は光子対モード $(a1,b2)$ か，または光子対モード $(a2,b1)$ のどちらかの光子対モードに見いだされることになるだろう．そこで図 3.4 中のビームスプリッタ (BS) の前では，光子対の状態は

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[e^{i\phi_b}|a\rangle_1|b\rangle_2 + e^{i\phi_a}|a\rangle_2|b\rangle_1\right] \tag{3.12}$$

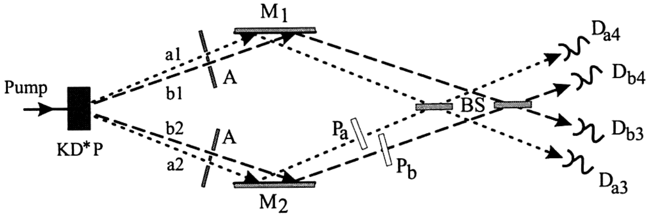


図 **3.4**　Rarity-Tapster によって提案された，タイプ I のパラメトリック下方変換により生じた光子対を利用した運動量のエンタングルメントについての実験系：開口 A によって互いに相関している二つの出射モードが選択される．その後，波長 a，波長 b のモードはそれぞれ別々のビームスプリッタによって重ね合わせられる．二つのビームスプリッタからの出力光子を測定するために検出器 $\mathrm{D_{a3}}$，$\mathrm{D_{b3}}$，$\mathrm{D_{a4}}$，$\mathrm{D_{b4}}$ が用いられている．$\mathrm{P_a}$，$\mathrm{P_b}$ は位相シフタを意味する

で表されるエンタングル状態になっている．むろん，このままの状態では二つの光子対モードは明らかに分離可能である．エンタングル状態は a モード同士および b モード同士をそれぞれビームスプリッタによって重ね合わせることによりはじめて得られる．これらのビームスプリッタの後では，それぞれの光子が上下のどちら光路を通ってきたのかをもはや区別できなくなるために，干渉が生じることになる．分岐比 50:50 のビームスプリッタの場合，上（下）から入力された状態 $|\mathrm{in}\rangle_1(|\mathrm{in}\rangle_2)$ はそれぞれ

$$|\mathrm{in}\rangle_1 \to \frac{1}{\sqrt{2}}\left[|\mathrm{out}\rangle_3 + i|\mathrm{out}\rangle_4\right] \tag{3.13}$$

$$|\mathrm{in}\rangle_2 \to \frac{1}{\sqrt{2}}\left[|\mathrm{out}\rangle_4 + i|\mathrm{out}\rangle_3\right]$$

に従って変換される．したがって，光子検出器 $\mathrm{D_{a4}}$, $\mathrm{D_{b4}}$, $\mathrm{D_{b3}}$, $\mathrm{D_{a3}}$ の前では光子対の状態は

$$\begin{aligned}|\Psi\rangle = \frac{1}{2}\Big[&(e^{i\phi_a} - e^{i\phi_b})|a\rangle_4|b\rangle_3 + (e^{i\phi_b} - e^{i\phi_a})|a\rangle_3|b\rangle_4 \\ &+ i(e^{i\phi_a} + e^{i\phi_b})|a\rangle_4|b\rangle_4 + i(e^{i\phi_a} + e^{i\phi_b})|a\rangle_3|b\rangle_3\Big]\end{aligned} \tag{3.14}$$

となることがわかる．こうして式中の右辺にある四つの項は，それぞれ異なる光子検出器の組み合わせによる同時計数の確率振幅に対応することになる．

同時計数率は干渉計の位相差 $\phi = \phi_a - \phi_b$ のシフトにともない，cos 関数に従って変化することがわかる．一方で，それぞれのビームスプリッタにおいてカラー a（またはカラー b）の光子による 1 光子干渉（1 次の干渉効果）が現れることはない．なぜならば，発生した二つの光子の位相の和はパラメトリック下方変換におけるエネルギー保存則のためにポンプ光の位相に一致しなければならないが，それぞれの光子自体は何ら確定した位相をもっておらず，光子対モード (a_1, b_2) に属するカラー a（またはカラー b）の光子と (a_2, b_1) に属する同じカラーの光子との間の位相は確定していないからである．

カラー a（またはカラー b）の干渉計の各々では，起こりうる二つの可能な自然放出過程の間の位相差をオフセット $\phi_a(\phi_b)$ がかかっている状態で測定しているともいえる．もし $\phi = \phi_a - \phi_b = 0$ であれば，二つの干渉計の出力の間には 100%の相関が現れ，$\phi = \pi/2$ であれば 100%の反相関が現れるはずである．この結果は，エンタングルした 2 光子の波動関数がもつ非局所的な性質を反映している．なぜならば，もし結晶から出た時点で光子の各々がすでにあらかじめ確定した位相をもっているのだと仮定するとこのような結果を説明することはできないからである．実験では 82%の可視度が観測されているが，この値は局所的実在を仮定した理論による最大予想値を超えている [94]．とはいえ，光軸調整および四つのモード間の重なりという実験上の困難のために，達成された干渉の可視度の値は，後述する偏光エンタングルメントの実験と比べて低い値にとどまっている．

3.4.4 偏光についてのエンタングルメント

平行ではない二つの光子ビームを出力するタイプ II の位相整合を用いることで，新しいタイプのエンタングル光子対をパラメトリック下方変換によって作り出すことができる [16]．図 3.5 と図 3.6 に示すように，ポンプ光の方向が複屈折結晶の光学軸となす角度を適切に調整すると，発生する二つの光子の放射コーンの各々が異なる中心軸をもつようになる．二つの放射コーンはそれぞれ常光線と異常光線に対応しており，二つの特別な方向に沿って放射の方向が重なることになる．ここでタイプ II の下方変換では，発生した二つの光子の偏光状態は常に直交していたことを思い出そう．このことから，この二つの特別な放射方向に関する限り光子は偏光をもたないことがわかる．なぜならば，光子は常光線モードに属しつつ同時に異常光線モードにも属し

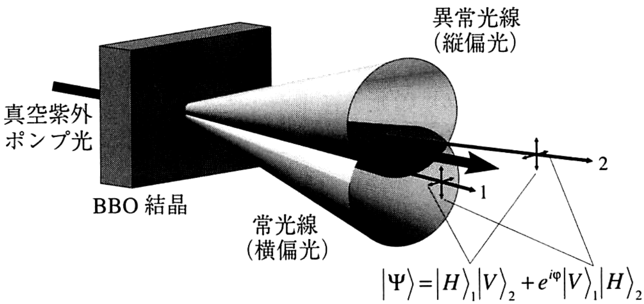


図 3.5　非平行な二つの光子ビームを出力するタイプ II のパラメトリック下方変換を利用して，波長の決まった互いに重なり合う二つの光の出射コーンを作り出すことができる．出射される光子は広いスペクトルをもっているが，偏光についてのエンタングルメントを高めるために特定の波長成分だけを狭帯域光フィルタによって取り出している

ているからである．ただし常光線と異常光線の伝播速度の違いを考慮すると，光子の検出時刻の違いから二つのモードを区別できるので，このままではこの議論は正しくはない．しかし，このような伝播速度の違い "ウォークオフ" は，半分の厚さの同種の結晶を（光学軸を）90 度だけずらしてそれぞれの経路に挿入することで補償できる．このウォークオフ補償によって二つのモードはもはや区別不可能になり

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left[|\mathrm{V}\rangle_1|\mathrm{H}\rangle_2 + e^{i\varphi}|\mathrm{H}\rangle_1|\mathrm{V}\rangle_2\right] \tag{3.15}$$

で表される偏光エンタングル状態を得ることができる．さらに位相補償用の結晶を利用すると，式 (3.15) の右辺における二つの項の間の位相 φ を操作できる．また，どちらかのビームに半波長板を入れると四つのベル状態の中の他の二つの状態

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left[|\mathrm{V}\rangle_1|\mathrm{V}\rangle_2 \pm |\mathrm{H}\rangle_1|\mathrm{H}\rangle_2\right] \tag{3.16}$$

を作り出すこともできる．上記の二つのベル状態における量子干渉の効果を見るためには，垂直偏光と水平偏光とを区別できなくなるような偏光の基底を選択しなければならない．これは単に偏光子を 45 度回すだけで容易に実現できる．

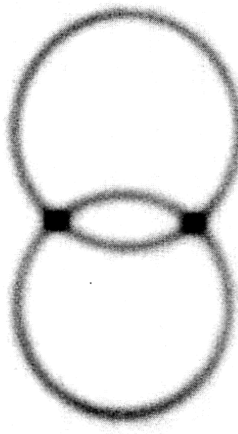


図 3.6 狭帯域光フィルタによって取り出した後の光子の出射コーンを示す図．二つのリングは常光線と異常光線に対応している．二つのリングが交差している方向では光子は偏光をもたない

3.5 ベル状態測定器

(*D. Bouwmeester, H. Weinfurter, A. Zeilinger*)

ベル状態測定は量子稠密符号化や量子テレポーテーションにおいて不可欠な要素であるが，その意図するところは単純である．単に入力された 2 量子ビット系の状態を，測定によって式 (3.1)～(3.4) で定義されたベル状態のいずれかに射影するだけである．そしてこの実験を繰り返すことによって，各々のベル状態に見いだされる確率を求めればよい．ただし，ベル状態の具体的な定義は，対象となるエンタングルメントの種類によって異なっていることに注意しよう．3.8 節で後述されるように，単一光子の運動量の自由度と偏光との間にあるエンタングルメントに対しては，簡単な線形光学の方法の範囲内でも四つのベル状態への完全な射影が可能である．一方で，二つの光子の偏光に関するエンタングルメントを扱う場合には事情は複雑になり，これまでのところ，四つのベル状態の中の二つの状態への射影しか実現されておらず，残りの二つのベル状態を区別することはまだできていない．本節ではこの光学的手段による不完全（ではあるが重要な）ベル状態測定について考察

することにしよう．

3.5.1　ビームスプリッタにおける光子の統計性

偏光エンタングルメントに対する不完全ベル状態測定は，ビームスプリッタにおける2量子ビット系の量子統計性を利用したものである．その基本は，式(3.1)～(3.4)で定義された四つのベル状態の中で状態 $|\Psi^-\rangle_{12}$(3.2) だけが粒子1と粒子2の入れ替えに対して非対称であり，他の三つのベル状態は粒子の入れ替えに対して対称であることにある．状態 $|\Psi^-\rangle_{12}$ の場合には二つの量子ビットはあたかもフェルミ粒子のように振る舞い，他の三つの状態の場合にはボース粒子のように振る舞うであろう．これまでは量子ビットを担う粒子がフェルミ粒子であるかボース粒子であるかには注意を払ってこなかった．実際に四つのベル状態の定義（式(3.1)～(3.4)）は構成粒子がフェルミ粒子であるかボース粒子であるかには依存していない．これは，これらの定義式が2準位系としての各粒子の内部状態だけを記述したものであり，粒子系の量子状態の完全な記述にはなっていないためである．量子状態の完全な記述は，粒子系の空間的な状態についての記述を加えることではじめて可能になる．ここで空間的な状態も，(粒子の入れ替えに対して）対称もしくは反対称になりうることに注意しよう．そこで粒子がボース粒子の場合には，内部状態が $|\Psi^-\rangle_{12}$ であれば空間についての状態は反対称になる．同様に内部状態が他の三つの状態であれば，空間についての状態は対称になる．一方で粒子がフェルミ粒子であれば事情はまったく反対になる．

まずボース粒子の例として2光子系を考えよう．そして2光子系の内部自由度として偏光に関する四つのベル状態を想定する．当然のことながら2光子系の量子状態は対称でなければならない．二つの粒子のそれぞれが別々のポート（モード $|a\rangle$ ，モード $|b\rangle$）からビームスプリッタに入力されると，出力される（空間についての）状態は

$$|\Psi_A\rangle_{12} = \frac{1}{\sqrt{2}}(|a\rangle_1|b\rangle_2 - |b\rangle_1|a\rangle_2) \tag{3.17}$$

$$|\Psi_S\rangle_{12} = \frac{1}{\sqrt{2}}(|a\rangle_1|b\rangle_2 + |b\rangle_1|a\rangle_2) \tag{3.18}$$

のいずれかとなる．ここで $|\Psi_A\rangle_{12}$ と $|\Psi_S\rangle_{12}$ はそれぞれ反対称，対称である．

全状態についての対称性の要請から，2 光子系の状態は

$$|\Psi^+\rangle|\Psi_S\rangle, \quad |\Psi^-\rangle|\Psi_A\rangle, \quad |\Phi^+\rangle|\Psi_S\rangle, \ |\Phi^-\rangle|\Psi_S\rangle \tag{3.19}$$

でなければならない．空間についての外部状態が反対称である場合のみ，内部状態についても反対称となることに注意しよう．このような状態のみがビームスプリッタから非対称な状態として出力されることになる．これを示すには，ビームスプリッタは内部状態には影響を及ぼさないと仮定し，ビームスプリッタの変換演算子（アダマール変換）を外部状態に作用させればよい．

実際に変換

$$H|a\rangle = \frac{1}{\sqrt{2}}(|c\rangle + |d\rangle) \tag{3.20}$$

$$H|b\rangle = \frac{1}{\sqrt{2}}(|c\rangle - |d\rangle) \tag{3.21}$$

を用いると

$$H|\Psi_A\rangle_{12} = \frac{1}{\sqrt{2}}(|c\rangle_1|d\rangle_2 - |d\rangle_1|c\rangle_2) = |\Psi_A\rangle_{12} \tag{3.22}$$

を示すことができる．

このように，空間について反対称な状態 $|\Psi_A\rangle_{12}$ はビームスプリッタ演算子の固有状態になっている [95,96]．それとは異なり，空間について対称な三つの状態では，二つの光子はビームスプリッタのどちらかのポートから一緒になって出力される．したがって，ベル状態 $|\Psi^-\rangle$ を残りの三つのベル状態から明らかに区別できる．なぜならば，状態 $|\Psi^-\rangle$ の場合に限って異なる出力ポート間での同時計数が得られるからである [97]–[99]．それでは残りの三つの状態を区別することは可能であろうか．ここで，状態 $|\Psi^+\rangle$ では二つの光子の偏光が異なっていることに注意しよう．$|\Phi^+\rangle$ と $|\Phi^-\rangle$ では，二つの光子の偏光は平行である．そこでビームスプリッタのそれぞれの出力ポートにおいて引き続き偏光分離を行えば，状態 $|\Psi^+\rangle$ を状態 $|\Phi^+\rangle$ と $|\Phi^-\rangle$ とから区別することができる．

ここまでの議論を同様な方針に従って一般化すれば，最大にエンタングルした四つの状態のうちの二つまでを互いに区別できることが示される．なぜならば，局所的なユニタリ変換によって 2 次元ヒルベルト空間での任意の回転操作を実行できるからである．

最後に粒子がフェルミ粒子だったらどうなるかを考察しよう [100]．この場合でもベル状態は依然として内部状態を記述する．たとえば，もし二つの量子ビットがスピンについてエンタングルしていれば，全量子状態についての非対称性の要請から四つの可能な状態は

$$|\Psi^+\rangle|\Psi_A\rangle, \quad |\Psi^-\rangle|\Psi_S\rangle, \quad |\Phi^+\rangle|\Psi_A\rangle, \text{ and } |\Phi^-\rangle|\Psi_A\rangle \tag{3.23}$$

となる．フェルミ粒子に対しては一つの状態だけが空間について対称であり，残りの三つは反対称である．こうして，状態 $|\Psi^-\rangle$ の場合に限って二つのフェルミ粒子は同一のポートから対になって出力されるため，残る三つの状態からの識別が可能である．他の三つの場合には二つのフェルミ粒子は異なるポートから出力される．

3.6　光子の量子ビットによる量子稠密符号化の実験

3.2 節で概観した量子稠密符号化を量子光学的な方法によって実現するためには [75]，図 3.7 に示すように，三つの構成要素，すなわちエンタングルした光子系を発生する粒子源，ボブによる光子への符号化を可能にするユニタリ変換光学系（符号化装置），ボブによって符号化された信号をアリスが読み出すために用いるベル状態測定器が必要である．偏光についてエンタングルした光子対は 3.4.4 項で説明したようにタイプ II のパラメトリック下方変換によって発生できる．ここではアルゴンレーザから出た波長 351nm の真空紫外光の光子を互いに直交する偏光をもつ波長 702nm の二つの光子の対へと変換している．

二つの特定な方向に沿って取り出した光子ビームに対して，BBO 結晶中で生じた複屈折の効果を補償するとエンタングル状態 $|\Psi^+\rangle$ を得ることができる．ここで，結晶から 1.5m 離れた場所で径 2mm のアイリスを入れることによって光子ビームの取り出し方向を慎重に選択している．片方の光子ビームはボブの符号化装置へと導かれ，他方の光子ビームはアリスのベル状態測定器へと導かれる．不完全ベル状態測定を可能にするために，二つの光子ビームの光路長差を，光可変遅延素子によって，それぞれの光子のコヒーレンス長 ($\ell_c \approx 100\,\mu$m) よりも短くなるように調整している．

偏光状態に符号化を施すためには，光子の偏光を変化させるための半波長

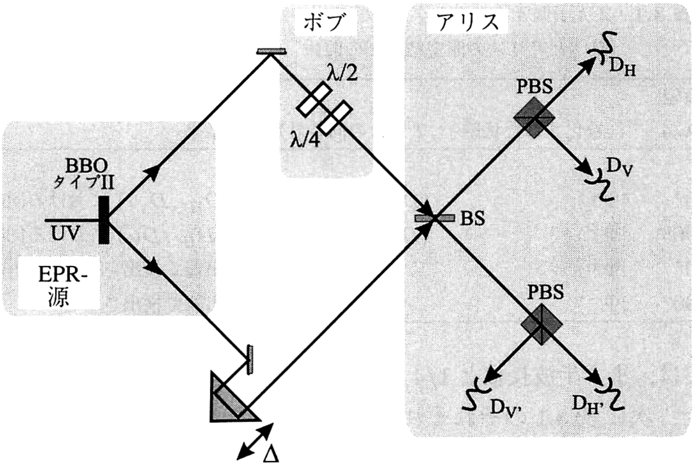


図 **3.7** 量子稠密符号化の光学実験系 [75]

板と，偏光に依存した位相シフトを与えるための 1/4 波長板が必要になる[2]．アリスの光子ビームは，ボブによる符号化を経たもう一つの光子ビームとベル状態測定器において重ね合わせられる．ここでベル状態測定器は，それぞれの出力ポートに偏光分離素子を備えたビームスプリッタと，偏光分離された光子を検出して同時計数を行うための四つの光子検出器とから構成されている．

ベル状態 $|\Psi^-\rangle$ だけが空間について反対称な状態であるため，ビームスプリッタの異なる出力ポート間での同時計数が記録されることになる（D_H と $D_{V'}$ での同時計数，もしくは $D_{H'}$ と D_V での同時計数）．残りの三つのベル状態に対しては，二つの光子はビームスプリッタのいずれか一方のポートから対になって一緒に出力される．状態 $|\Psi^+\rangle$ は二つの光子の偏光が異なっているために他の二つの状態から容易に区別できる．実際，状態 $|\Psi^+\rangle$ の場合には，同一の出力ポートにおいて，しかし異なる偏光成分の間での同時計数が記録される（D_H と D_V での同時計数，もしくは $D_{H'}$ と $D_{V'}$ での同時計数）．$|\Phi^+\rangle$ と $|\Phi^-\rangle$ の場合には，二つの光子は一緒に同じ検出器に導かれるために，これら二つの状態を区別することはできない．表 3.1 はボブによる符号化操作とアリスによる同時計数の結果との間にある対応関係をまとめたものである．

[2] 1/4 波長板の光学軸に平行な偏光成分は垂直な偏光成分に対して位相にして $\pi/2$ だけシフトする．光学軸を垂直から水平に変更すると水平偏光成分と垂直偏光成分との間の位相変化は π となる．

表 3.1　2光子偏光エンタングル状態を用いた量子稠密符号化実験：ボブの操作とアリスの測定結果との関係

ボブの設定 $\lambda/2$	$\lambda/4$	符号化された状態	アリスの同時計数測定結果
0°	0°	$\|\Psi^+\rangle$	(D_H, D_V) もしくは $(D_{H'}, D_{V'})$ における同時計数
0°	90°	$\|\Psi^-\rangle$	$(D_H, D_{V'})$ もしくは $(D_{H'}, D_V)$ における同時計数
45°	0°	$\|\Phi^+\rangle$	二つの光子が同一の検出器で検出される
45°	90°	$\|\Phi^-\rangle$	二つの光子が同一の検出器で検出される

実験では，まず半波長板と1/4波長板の両方を垂直配置にして状態 $|\Psi^+\rangle$ を準備した．次に表3.1のそれぞれの手順に従って順次他の三つのベル状態に変換した．ここでアリスのベル状態測定器において2光子干渉を観測するために，二つの光子ビームの光路長差 Δ を可変光遅延素子によって変化させている．光路長差 Δ がコヒーレンス長 l_c よりも長いときには干渉は現れず，検出器の同時計数には古典的な統計性が見られるだけである．

図3.8と図3.9は，検出器 $H-V$ 間 $(C_{HV}(\bullet))$ および検出器 $H-V'$ 間 $(C_{HV'}(\circ))$ での同時計数率が光路長差の変化に伴ってどのように変化するのかを，状態 $|\Psi^+\rangle$ と $|\Psi^-\rangle$ の各々に対して調べた実験結果である．$C_{HV}(\bullet)$ の値は，光路長差が0のときに状態 $|\Psi^+\rangle$ に対しては最大となり（図3.8参照），状態 $|\Psi^-\rangle$ に対しては最小となる（図3.9参照）．一方で $C_{HV'}(\circ)$ の値はまったく逆の様相を示しており，状態 $|\Psi^-\rangle$ の特徴を如実に表している．これらの実験結果から，もし二つの光子の両方を検出できたときには95%および93%の信頼性でそれぞれ $|\Psi^+\rangle$ と $|\Psi^-\rangle$ とを特定できることになる．

単一光子検出のためにシリコン・アバランシュ・ダイオードをガイガーモードで使う場合には，ベル状態測定器のさらなる工夫が必要である．状態 $|\Phi^+\rangle$ または $|\Phi^-\rangle$ を（状態 $|\Psi^+\rangle$ と $|\Psi^-\rangle$ とから）識別するためには一つの検出器で二つの光子の到来を検出しなければならないからである[3]．

状態 $|\Phi^+\rangle$ および $|\Phi^-\rangle$ に対してはそもそも2光子干渉が生じないように工夫する，という方法もある．それぞれの光路に厚めの水晶板を挿入して異な

[3] 1光子の到来と2光子の到来とを識別できる必要がある．シリコン・アバランシュ・フォトダイオード単体では一光子の到来と2個以上の光子の到来とを区別できないので，2光子の到来を検知するには二つの検出器の間での同時計数に頼るしかない．特殊な光電子増倍管を使うとこれらの識別はできるが，現在のところ検出効率は非常に小さい．

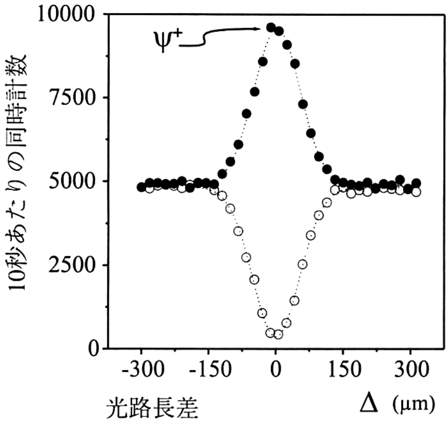


図 3.8 光路長差 Δ の関数として同時計数率 C_{HV} (•) と $C_{HV'}$ (○) を測定した結果（送られた状態は $|\Psi^+\rangle$）．$\Delta = 0$ の場合には C_{HV} に干渉による強め合いが見られ，$|\Psi^+\rangle$ が送られたことがわかる

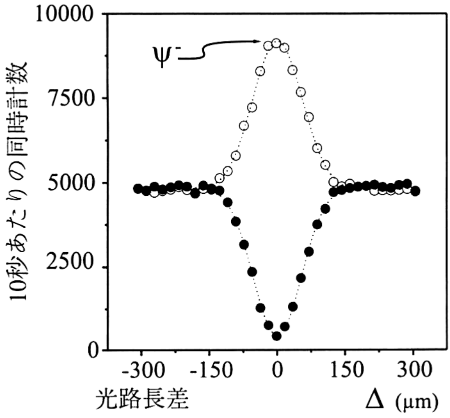


図 3.9 光路長差 Δ の関数として同時計数率 C_{HV} (•) と $C_{HV'}$ (○) を測定した結果（送られた状態は $|\Psi^-\rangle$）．干渉による強め合いが $C_{HV'}$ に見られ，$|\Psi^-\rangle$ が送られたことがわかる

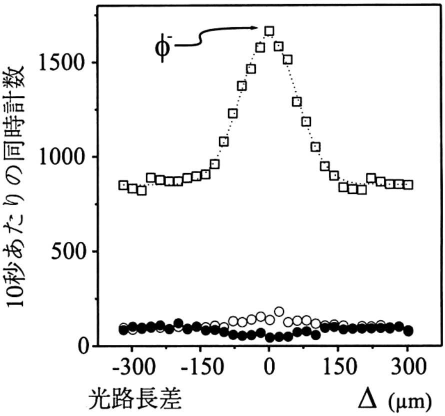


図 3.10　光路長差 Δ の関数として同時計数率 $C_{H\overline{H}}$ (□), C_{HV}(•), $C_{HV'}$ (○) を測定した結果．$C_{H\overline{H}}$ におけるピークは状態 $|\Phi^-\rangle$ によるものである． $C_{H\overline{H}}$ の計数率は図 3.8 や図 3.9 と比べて 1/4 程度になっている（この理由については本文を参照）

る偏光成分の間にコヒーレンス長 ℓ_c 以上の伝播遅延が出るようにすればよい．一方の経路では $|H\rangle$ 成分を，他方の経路では $|V\rangle$ 成分を遅延させるのである（状態 $|\Psi^+\rangle$ と $|\Psi^-\rangle$ に対しては 2 光子干渉が生じることに注意）．別の方法としては，同じ出力モード中に存在する二つの光子を付加的なビームスプリッタによってさらに分離し，それぞれの出力ポートの間での同時計数を行うことが考えられる（同時計数が得られる確率は 50%ではあるが）．この方法の有効性を確かめるために，実験では検出器 D_H の置かれた出力ポートに対してのみ上記の構成を取り入れた．ここで新たに加えられた検出器を $D_{\overline{H}}$ とする．ボブが状態 $|\Phi^-\rangle$ を選んだ場合，光路長差が 0 のときには検出器 D_H と $D_{\overline{H}}$ の間の同時計数率 $C_{H\overline{H}}$(□) の値が増大するのに対し，同時計数率 C_{HV} と $C_{HV'}$ の値は一定の背景レベルに保たれることを図 3.10 は示している．ただし，光子対の半数は依然として同じ検出器に導かれる上に付加的なビームスプリッタによるさらなるモード分離は一箇所でしか行っていない．そのため同時計数率 $C_{H\overline{H}}$ の最大値は，C_{HV}（図 3.8）や $C_{HV'}$（図 3.9）の最大値の 1/4 にとどまらざるを得ない．

このようにすれば，ともかく 3 種類のメッセージを区別することが可能になるので，いまやボブの符号化装置は量子稠密符号化のための装置として機

文字種	K					M					°				
ASCII コード	75					77					179				
トリット	0	2	2	1	0	0	2	2	1	2	2	0	1	2	2

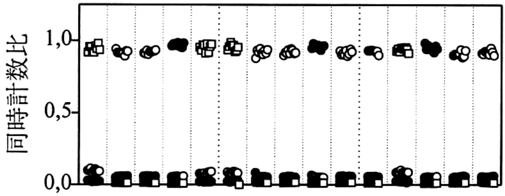


図 3.11 光子当たり 1.58 ビットを符号化した量子稠密符号化通信の実験：文字列 “KM°” の ASCII コード（つまり 75, 77, 179）を通常の 24 ビットではなく 15 トリットに符号化している．ここで “0”≡ $|\Phi^-\rangle \mathrel{\widehat{=}} \square$, “1”≡ $|\Psi^+\rangle \mathrel{\widehat{=}} \bullet$, “2”≡ $|\Psi^-\rangle \mathrel{\widehat{=}} \circ$) としている．それぞれのデータはそれぞれの最大計数率によって規格化されていることに注意しよう

能しうる．ASCII コードでの KM° (75, 77, 179) を 24 ビットの代わりに 15 トリットで符号化して送信した場合の各々のトリットに対する同時計数率の実験結果を図 3.11 に示そう．ここで，それぞれの実験値は送信された状態における最大同時計数率によって規格化されている．この測定結果を元にして送信された状態に対応する同時計数率と他の二つの状態による同時計数率とを比べれば信号雑音比 (S/N) を評価することができる．三つの状態 $|\Psi^+\rangle$, $|\Psi^-\rangle$, $|\Phi^-\rangle$ に対する S/N は，それぞれの干渉における可視度の違いのために異なっており，それぞれ 14.8, 13.0, 8.5 となっている．

3.7 光子の量子ビットに対する量子テレポーテーションの実験

(*D. Bouwmeester, J.-W. Pan, H. Weinfurter, A. Zeilinger*)

本節では，光子の偏光状態に符号化された量子ビットに対する量子テレポーテーションの実験について説明しよう [76]．テレポートされる偏光状態を担っている光子を光子 1 とし，光子 2 と光子 3 は互いに偏光についてエンタングルした光子対を形成しているとする．量子テレポーテーションでは，光子 1 の

初期偏光状態が光子3の上に再生されるようにしなければならない．図3.12は実験系の概略図である．3.3節で述べたように，量子テレポーテーションの実現のためにはエンタングル状態の生成（Einstein-Podolsky-Rosen(EPR) 対の生成）とベル状態測定 (BSM) が必要不可欠であるが，偏光についてエンタングルしている光子対の生成方法については3.4節ですでに述べた．また，状態 $|\Psi^-\rangle$ を識別するベル状態測定器についてもすでに3.5節で説明済みである．

ここでは範囲を限定して，実験で用いるベル状態測定器は状態 $|\Psi^-\rangle$ だけを識別できれば十分であるとしよう[4]．したがって，ベル状態測定の結果，アリスが状態 $|\Psi^-\rangle$ を得た場合には，ボブの手元にある光子3の状態はベル状態測定を行う前の光子1と同じ状態にあるはずである．

検出器への到着時刻の違いのために光子1と光子2が識別可能になり，ベル状態測定が成立しなくなってしまうのを避けるために，以下に述べるような実験上の工夫が必要である．図3.12に示すように，パルス化されたポンプ光子からのパラメトリック下方変換によって互いにエンタングルした光子2と光子3の対が生成される．通常，パルス幅が100フェムト秒になるようにモードロックされたチタン・サファイア・レーザからの出力光から生成された倍高調波をポンプ光として用いている．パルス化されたポンプ光は結晶のすぐ後で反射され，結晶中を逆行中にさらなる光子対（光子1と光子4）を作り出す．ここで光子4は光子1の存在を検知するためのトリガーとして利用される．こうして光子1と光子2は200フェムト秒程度の時間幅の中に共存することになる．さらに遅延を調整すればこれらの二つの光子の時間的な重なりを大きくできる．とはいえ，光子1と光子2に対する時間軸上での識別不可能性がこれで保証されたわけではまだない．なぜならば，下方変換によって発生した光子のコヒーレンス時間幅は50フェムト秒程度であり，ポンプ光のパルス幅よりもかなり短いからである．こうした事情のため，これら四つの光子に対して同時計数を行うためには50フェムト秒を上回る時間分解能が要求される．そこで実験では，それぞれの光子の波束の時間幅を広げてポンプ・パルス光の時間幅よりもかなり長くなるように変形し，時間軸上でこれらの光子が識別不可能になるようにしている．幅4nmの狭帯域干渉フィルタを検出器の前に挿入することで，光子の波束は500フェムト秒程度まで

[4] もちろん3.5節で説明したように状態 $|\Psi^-\rangle$ と $|\Psi^+\rangle$ の識別は可能である．

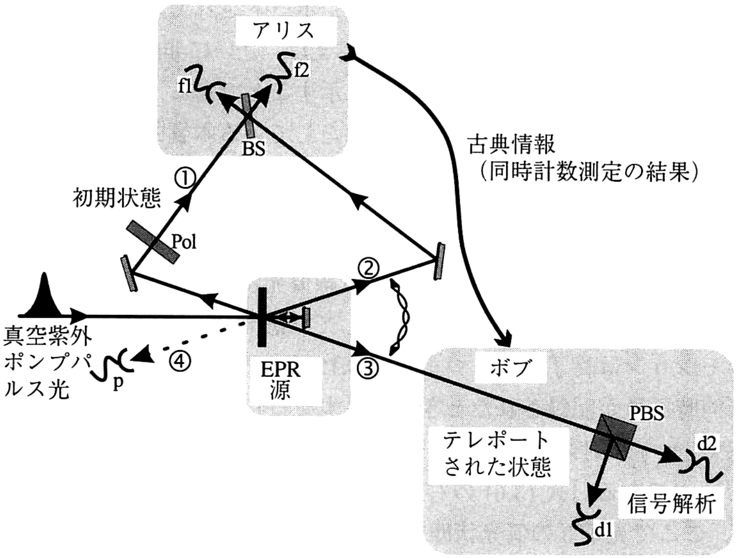


図 3.12 光子の量子ビットに対する量子テレポーテーションの実験系の構成：非線形光学結晶を通過する真空紫外のパルス光は互いにエンタングルした光子 2 と光子 3 を作り出す．さらに，結晶中を逆行するときにパルス光はまた別の光子対（光子 1 と光子 4）を作り出す．そのうち光子 1 は転送されるべき量子状態に準備される．光子 4 は光子 1 の存在を示すトリガーとして利用される．光子 1 と光子 2 が重ね合わされたビームスプリッタにおいて，アリスは検出器 f1 と f2 の同時計数を観測する（このとき，ベル状態測定の結果は $|\Psi^-\rangle_{12}$ である）．アリスから同時計数が観測されたことを告げられた時点で，ボブは光子 3 の状態が光子 1 の初期状態になっていることを知る．これを確認するには光子 3 に対して偏光分離 (PBS) を行い，どちらのポートで光子を検出するか（d1 か d2 か）を測定すればよい．検出器 P における光子 4 の検出は光子 1 の存在を示すことになる

引き延ばされ，光子1と光子2に対する識別不可能性の度合は最大85%にまで改善されている [101].

量子テレポーテーションを実現するために必要な実験系の説明はこれで終わりである．しかし未知の量子状態がテレポートされていることをどのようにして検証すればよいのだろうか．その答えは，互いに非直交な二つの既知の量子状態が共にテレポート可能なことを示すことである．量子テレポーテーションにおいてエンタングルメントが果たしている本質的な役割を明らかにするためには，このように非直交な量子状態の組を用いた検証が必要になる．

3.7.1　実験結果

最初に光子1の量子ビットは45度の直線偏光状態に準備される．光子1と光子2に対するベル状態測定の結果として状態 $|\Psi^-\rangle$ が得られれば量子テレポーテーションは終了する．つまり図3.12中の二つの光子検出器 f1 と f2 において同時計数が記録されたときには（すなわち，光子1と光子2の状態がベル状態 $|\Psi^-\rangle$ に射影されたとき），光子3は45度の直線偏光状態に見いだされるはずである（式(3.6)の右辺第1項の全体にかかる負符号は重要ではない）．ここで光子3の偏光状態を調べるには +45度と −45度の直線偏光を分離する偏光分離素子を用いればよい．テレポーテーションが行われたことを示すには，f1 と f2 との間での同時計数が記録された場合には光子3は +45度の出力ポートの後に置かれた検出器 d2 でしか検出されないことを確かめればよい．一方で，−45度の出力ポートの後に置かれた検出器 d1 において光子3が検出されてはならない．したがって，三つの検出器に対する同時計数 d2f1f2（+45度偏光の検出）を記録した場合には，同時計数 d1f1f2（−45度偏光の検出）は決して記録されないことが確認できれば，光子1の初期偏光状態（量子ビットの初期状態）が光子3へとテレポートされたことを結論できる．

光子1と光子2に対する識別不可能性を保証するために，非線形光学結晶とその後にある反射鏡との間の距離を調整して光子1と光子2が同時にビームスプリッタに到着するようにする（遅延の制御）．もしこれらの光子が時間軸上で重なっていれば，量子テレポーテーションが起こっているはずである．

もし光子1と光子2が時間軸上で重なっていなければ，それぞれの光子は相手がどう振る舞うかとは無関係に f1 か f2 のどちらかの検出器に入ること

になる．この場合，f1 と f2 との間の同時計数の確率は 50%になる[5]．この値は時間軸上での重なりがある場合に得られる同時計数の確率の 2 倍であることに注意しよう．なぜならば後者の場合，状態 $|\Psi^-\rangle$ が得られたときにのみ同時計数が記録されるからである（ベル状態測定により $|\Psi^-\rangle$ が得られる確率は 1/4(25%) であることを思い出そう）．光子 2 は偏光エンタングルメントをもつ光子対の片割れであり，それ自体は何ら定まった偏光状態をもっていない．そして光子 1 の偏光状態とは無関係に，光子 1 と光子 2 の直積状態は四つのベル状態の等確率振幅の重ね合わせ状態で記述できる．光子 2 と同様に光子 3 もまた何ら確定した偏光状態をもっていない．それゆえ検出器 d1 と d2 はそれぞれ確率 50%で光子 3 を検出することになる．以上の考察から，光子 1 と光子 2 が時間軸上で重なっていない場合には，同時計数 d1f1f2（−45 度偏光の検出）もしくは同時計数 d2f1f2（+45 度偏光の検出）が記録される確率はそれぞれ 25%になることが導かれる．

図 3.13 は（光子 1 と光子 2 の間の）遅延の関数として同時計数 d1f1f2（−45 度偏光）と同時計数 d2f1f2（+45 度偏光）の率を計算したものである．図 3.13(a) に見るように，遅延が 0 のときに同時計数 d1f1f2（−45 度偏光の検出）が 0 まで減少していることから，+45 度の直線偏光状態の量子テレポーテーションに成功したことが裏付けられる．一方で，図 3.13(b) に見るように，同時計数 d2f1f2（+45 度偏光）の値は遅延によらずに一定である．もちろん，これらの理論的予測は検出器 P においてトリガー光子（光子 4）を検出したという前提のもとで導かれたものであることに注意しよう．

図 3.14 の左側のパネルに，+45 度の直線偏光をもつ光子に対する量子テレポーテーションの実験結果を示す．図 3.14(a) と (b) をそれぞれ図 3.13 に示された理論値と比べてみよう．−45 度における曲線に顕著なくぼみが見られること，および +45 度に対しては同時計数はほぼ一定になることから，光子 3 の偏光状態は光子 1 の初期偏光状態と同じであることが示唆される．これらの結果は，量子テレポーテーションの過程によって説明が可能である．

ここで，三つの光子ではなく実際には四つの光子に対する同時計数を行っていることを強調しておこう．なぜならば光子 4 を光子 1 の存在を保証するためのトリガーとして利用しているからである．

---

[5] 訳注：光子検出器の分解可能時間は光子波束の時間幅に比べるとはるかに長いことに注意．

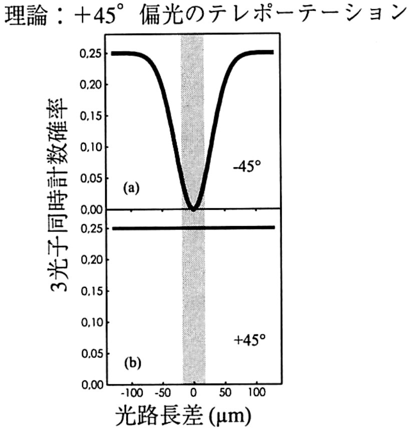


図 3.13　検出器 f1，f2（これらはベル状態 $|\Psi^-\rangle$ を測定する）と光子 3 を検出する検出器との間での 3 光子同時計数確率についての理論予測：光路長差が 0 の位置で 3 光子同時計数 (d1f1f2) の値が 0 になること (a)，他方で 3 光子同時計数 (d2f1f2) の値は光路長差によらず一定であること (b) から +45 度の直線偏光状態が光子 1 から光子 3 にテレポートされたことが証拠づけられる

得られた実験結果に対するあらゆる可能な古典物理学的な解釈を排除するために，さらに +90 度の直線偏光状態に対するテレポーテーションの実験を行わなければならない．ここで +90 度の直線偏光は +45 度の状態とは非直交であることに注意しよう．実験結果を図 3.14(c) と (d) に示す．0 度における曲線のくぼみの深さから 70%±3%の可視度が得られているのがわかる．

図 3.14 の実験結果から，単一光子の偏光に符号化された量子ビットに対する量子テレポーテーションの忠実度を評価することができる．ここで忠実度は，入力された量子ビットと出力された量子ビットとの間の重なりの度合として定義される．図 3.15 にその評価値をプロットしてみた．この実験では，テレポートされた量子ビットが特定の検出器 d2 にのみ導かれるように設定しているが，これは次の二つの意味がある．その一つは量子ビット（光子 1）が入力された場合に得られるであろうイベントだけを抽出することであり，もう一つはテレポーテーションにおける忠実度を測定することである．

最後に次のような事情に留意しておこう．パルス化されたポンプ光が結晶中を逆行するときに光子対をたまたま二つ生成すると，ベル状態測定器によっ

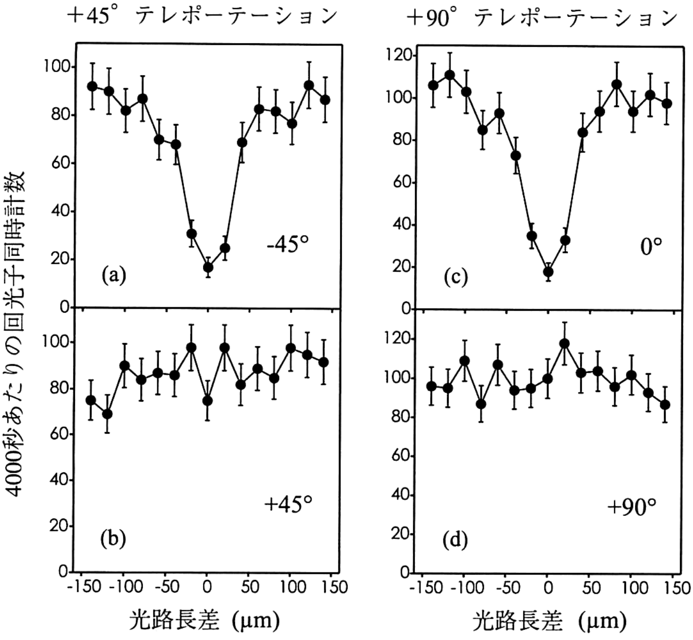


図 3.14 光子の量子ビットに対するテレポーテーションの実験結果：((a) と (b)）光子 1 の初期状態は +45 度の直線偏光，(a) は 3 光子同時計数 d1f1f2（−45 度），(b) は 3 光子同時計数 d2f1f2（+45 度）；((c) と (d)）光子 1 の初期状態は +90 度の直線偏光，(a) は 3 光子同時計数 d1f1f2（0 度），(b) は 3 光子同時計数 d2f1f2（+90 度）．これらの 3 光子同時計数結果は，検出器 P でも同時に光子 4 が検出されたという条件のもとで抽出されたものである（つまり実際には 4 光子同時計数を行っている）．図の横軸は光子 1 と光子 2 との光路長差である（図 3.12 参照）．これらの実験結果から，任意の量子ビット状態に対する量子テレポーテーションの成立が確かめられる

て二つの光子が検出されることがありうる．この場合にはボブによって光子が検出されることはなく [83]，二つの光子が検出器 P に入ることになる．このような解析上望ましくないイベントは，光子 1 個の到来と 2 個の到来とを区別できるような検出器を P に適用すれば除外できる [102].

このような特殊な検出器を用いるか否かにかかわらず，測定される忠実度の値は同じであろう [84]．なぜならば，忠実度はアリスのベル状態測定器に

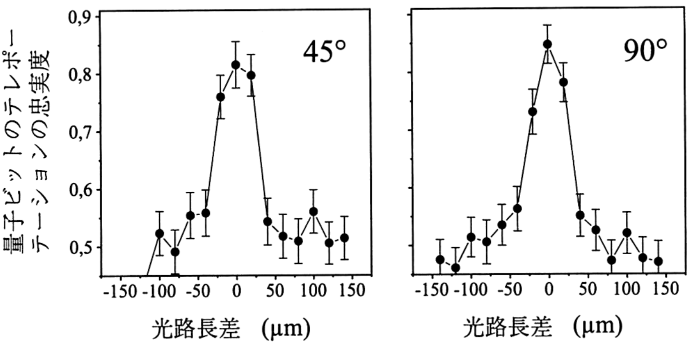


図 3.15　単一光子の偏光状態に符号化された量子ビットに対する量子テレポーテーションにおける忠実度：4 光子同時計数の方法によって測定された入力量子ビットと出力量子ビットとの間の重なり合いの度合は最大 80%である

おいて検出された二つの光子に対する識別不可能性の度合によって基本的に決まってしまうからである．識別不可能性の度合はパルス化されたポンプ光の周波数帯域幅と干渉フィルタの帯域幅の比に直接関係している．この比が大きければ高い忠実度が得られるし，小さければ低い忠実度しか得られない．

3.7.2　エンタングルメントに対するテレポーテーション

3.7.1 項の量子テレポーテーション実験では，光子 4 は光子 1 の存在を示すトリガーの役割をはたしていた．さらに図 3.16 に示すように，光子 4 が光子 1 とエンタングル状態 $|\Psi^-\rangle$ にあることを考慮すれば，光子 4 に別の役割をもたせることができる．

光子 1 それ自体は確定した量子状態をもたず，すべての情報は光子 4 との間のエンタングルメントに含まれている．もしここで前節と同様に光子 1 の量子ビットに対して量子テレポーテーションを行うと，光子 1 に付随する性質は光子 3 にそのまま移されることになる．すなわち図 3.16 に示すように，今度は光子 3 と光子 4 とがエンタングルすることになる．もとはといえば光子 3 と光子 4 はそれぞれ別々の光源から発生したものであり，両者の間に直接の相互作用はまったくない．それにもかかわらず，興味深いことに，量子テレポーテーションの後ではそれらの二つの光子がエンタングルできるのである．このようなエンタングルメントそのもののテレポーテーション [86] は

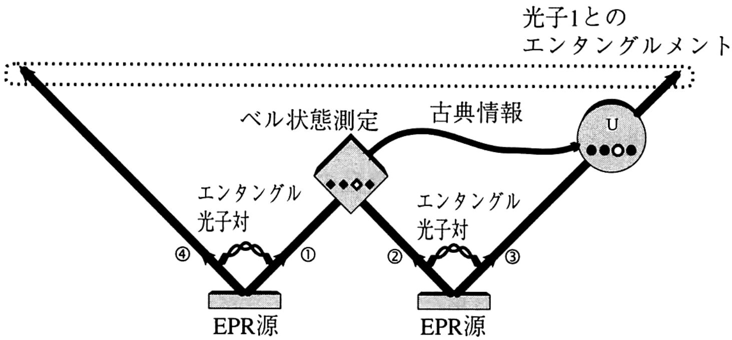


図 3.16　エンタングルメント・スワッピングの基本原理：二つの EPR 粒子源のそれぞれによってエンタングルした光子対（光子 1–光子 4），（光子 2–光子 3）を作り出す．次に光子 1 と光子 2 に対してベル状態測定 (BSM) を行う．この測定の結果，光子 3 と光子 4 は新たにエンタングル状態になる

エンタングルメント・スワッピングと呼ばれており，3.10 節および 3.11 節で紹介するように，これを用いたいくつかの興味深い利用方法が提唱されている［85,87］.

3.7.3　まとめと展望

偏光エンタングルメントをもつ光子の対を二つ用意できれば，2 光子干渉の方法を用いることで，一つの光子の偏光状態に符号化された量子ビットを別の光子の上に移すことができる．続く二つの節で見るように，光学的な方法で量子テレポーテーションを行う方法は他にも存在する．しかし，ここではむしろ量子テレポーテーションの実現が光学的な手段にのみ限定されているわけではないことを強調しておきたい．光子の対の代わりにエンタングルしている原子の対を利用したり [103]，光子と原子・イオンとの間にエンタングルメントを形成することも原理的には可能である．これらをうまく利用できれば，デコヒーレンスが速くて寿命の短い粒子の量子状態をより安定度の高い別の物理系の上に移すことが可能になるだろう．光子の入力情報を，環境から注意深く遮断されてトラップされているイオンや原子の上に記録すれば量子メモリができるかもしれない．

さらに 8 章のテーマであるエンタングルメント精製 [49] を実行して，あら

かじめ二つの場所の間で質の高い量子エンタングルメントを準備しておくことができれば，仮に粒子を直接に送ると擾乱の影響によって量子状態が壊れてしまうことを免れないような場合でも，何ら量子状態を壊すことなくある場所から別の場所へと量子状態を移すことが可能になる．2地点間の距離が量子状態を直接送るには長すぎて（擾乱の度合が大きくなりすぎるために）標準的なエンタングルメント精製が実行できないような場合には，2地点間をいくつかの区間に細分化した後でそれぞれの区間においてエンタングルメント精製を実行してから，最後に次々とエンタングルメント・スワッピングを行えばよい．これは量子中継[104]と呼ばれる方法であり，8.7節で後述される．このように，環境との相互作用による擾乱の影響を回避しつつ量子状態を保持できるということは，量子通信や量子計算において非常に重要な意味をもっている．

3.8　二つの光子を利用した量子テレポーテーションの実験

(*D. Bouwmeester*)

はじめに3.3節で概観したように，量子テレポーテーションは二つの基本要素から構成されている．一つは量子通信路におけるエンタングルメントの利用であり，もう一つは測定結果に関する送信者からの古典情報の提供とそれに基づいた受信者による量子状態の再構成である．それぞれの基本要素は量子状態についてのいかなる情報も含んではおらず，両者を合わせることによってはじめて量子状態を別の場所に移すことができる．

3.7節では3光子もしくは4光子の同時計数実験によって量子テレポーテーションを行った．しかしこれらの実験は——アリスは完全なベル状態測定を行うことができない——という点である種の欠点を抱えている．つまり量子テレポーテーションの効率の低下が避けられない．完全なベル状態測定を行うためには二つの光子間の制御NOT演算に相当する相互作用が必要になるが，これを物理的に実現するのはいまのところ極めて困難である．これから紹介する方法はPopescu[77]により提案されローマ大学の実験グループ[78]によって実施されたもので，ベル状態測定の不完全性の問題は見事に回避されている．とはいうものの，テレポートの対象となる量子状態の準備にあたっ

て強い制限が課されることになる．

最初の量子テレポーテーションの提案では関与する粒子の個数は三つであった．そのうちの二つの粒子は互いにエンタングル（スピン 1 重項状態）しており，アリスとボブの間に非局所的な量子通信路を提供している．3 番めの粒子はアリスが所持しており，初期状態 Ψ にある．ここで 3 番めの粒子は，第三者によって状態 Ψ に準備されているか，アリスが自分で拾ってくるものと仮定されている（いずれにせよその量子状態はアリスにとって未知である）．これから解説する方法では，非局所量子通信路を構成している二つの粒子だけを利用する．第三者は量子状態 Ψ を 3 番めの粒子に符号化する代わりに，アリスの手元に届くであろう（スピン 1 重項状態にある光子対の）光子を途中で操作して状態 Ψ を符号化する．ここで符号化にあたっては，光子対にエンタングルメントをもたらしている自由度とは異なる別種の自由度を利用しなければならない．

このように設定を変えたとしても，符号化された量子状態 Ψ はアリスにとっては未知であることに注意しよう．したがって，もしアリスが古典通信路しか使えないのであれば，状態 Ψ をボブに伝えることはできない．しかし，これから示すようにアリスは非局所量子通信路を使って状態 Ψ をボブに量子テレポートすることができるのだ．

2 光子の方法では 3 光子の方法と比較してアリスの行う操作は簡単である．二つの異なる粒子を相互作用させることよりも，一つの粒子についての二つの異なる自由度を相互作用させることのほうがしばしば簡単で済むからである．

以下では，参考文献 [77] で提案された光学実験の各段階を追いながら，2 光子を用いた量子テレポーテーションの基本手順の説明を行うことにしよう．第 1 段階では伝播方向についてエンタングルした二つの光子（つまり運動量についてのエンタングルメント）を用意する．ただし，それぞれの光子は確定した偏光状態をもっているものとする．図 3.17 に，EPR 源を用いた実例を示す [78]．まず，タイプ II のパラメトリック下方変換によって偏光についてエンタングルしている状態を生成する．

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 + |V\rangle_1|H\rangle_2\right) \tag{3.24}$$

ここで添え字 1 と 2 は二つの相関した光子のそれぞれの出射方向を表してい

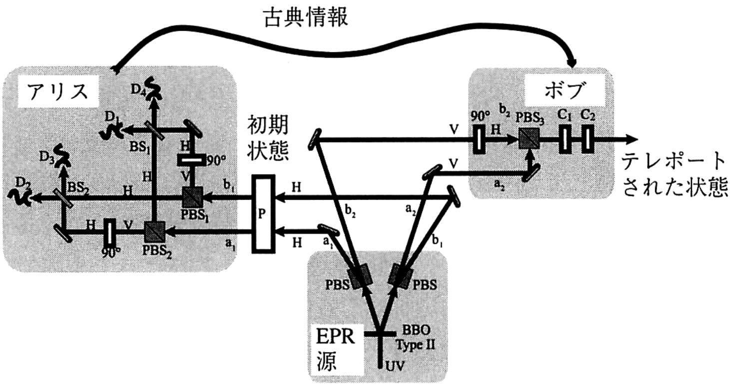


図 3.17　二つの光子を利用した量子テレポーテーションのための実験系：構成要素は以下のとおりである；偏光エンタングルメントをもつ光子対を作り出すためのタイプ II のパラメトリック下方変換結晶 (BBO)，水平と垂直直線偏光を分離するための偏光分離素子 (PBS)，分岐比 1:1 のビームスプリッタ (BS)，単一光子検出器 ($D_1 \sim D_4$)，90 度偏光回転素子，初期量子状態を準備するための光学系 (P)，偏光変換素子 (C)

る．続いてそれぞれの光子は偏光分離素子によって水平偏光成分と垂直偏光成分とに分離される．このようにして偏光エンタングルメントは運動量についてのエンタングルメントに変換される．

$$\frac{1}{\sqrt{2}}\left(|a_1\rangle|a_2\rangle + |b_1\rangle|b_2\rangle\right)|H\rangle_1|V\rangle_2 \tag{3.25}$$

ここで，添え字 1 と 2 はそれぞれアリスとボブに向かう二つの方向を表しており，アリスに向かう光子は水平偏光 H にあり，ボブに向かう光子は垂直偏光 V にあることに注意しよう．ここで運動量についてのエンタングルメントは非局所的な量子通信路を形成している．光子 1 の偏光状態は，アリスのもとに向かう途中で第三者 P によって水平偏光 H から任意の状態

$$|\Psi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1 \tag{3.26}$$

へと変換される．第三者 P は光子の経路 a_1 と b_1 の双方において同一の偏光操作を行う．状態 $|\Psi\rangle_1$ こそは，アリスがボブへとテレポートしたい（しかしアリスにとっては未知の）量子状態である．ここでは量子力学的な粒子がもっ

ている空間についての自由度と偏光についての自由度の両者を利用している点が重要である[6]．第三者Pによる偏光状態操作の後では2光子系の状態は

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|a_1\rangle|a_2\rangle + |b_1\rangle|b_2\rangle\right)|\Psi\rangle_1|V\rangle_2 \tag{3.27}$$

となる．これは式(3.6)における状態Ψ_{123}と形式的には同じ意味をもっている．

次に，光子1に対して，アリスは偏光状態$|\Psi\rangle_1$と経路に関する状態（経路a_1かb_1か）との間の結合測定（形式的にはベル状態測定に相当）を行う．光子1を偏光と運動量に関する四つのベル状態のいずれかに射影する方法があったと仮定しよう．すると式(3.6)との形式的な類似性から

$$\begin{aligned}|\Phi\rangle = \frac{1}{2}\ [\ &(|a_1\rangle|V\rangle_1 + |b_1\rangle|H\rangle_1)(\beta|a_2\rangle + \alpha|b_2\rangle)|V\rangle_2 \\ +\ &(|a_1\rangle|V\rangle_1 - |b_1\rangle|H\rangle_1)(\beta|a_2\rangle - \alpha|b_2\rangle)|V\rangle_2 \\ +\ &(|a_1\rangle|H\rangle_1 + |b_1\rangle|V\rangle_1)(\alpha|a_2\rangle + \beta|b_2\rangle)|V\rangle_2 \\ +\ &(|a_1\rangle|H\rangle_1 - |b_1\rangle|V\rangle_1)(\alpha|a_2\rangle - \beta|b_2\rangle)|V\rangle_2\ ]\end{aligned} \tag{3.28}$$

が得られる．右辺のそれぞれの項において最初の因子は光子1のベル状態に対応し，第2の因子は光子2の状態に対応している．三つの光子を用いる方式とは異なり，光子1の状態を四つのベル状態に射影することは困難な操作ではなく100%に近い効率で実現できる．まず，光子1において偏光自由度と空間についての自由度とをエンタングルさせなければならない．これは経路a_1とb_1のそれぞれにおいて偏光分離を行ってから，経路a_1から来るV偏光成分$(|a_1\rangle|V\rangle_1)$と経路b_1から来るH偏光成分$(|b_1\rangle|H\rangle_1)$とを結合させることにより可能である．同様に$(|a_1\rangle|H\rangle_1)$と$(|b_1\rangle|V\rangle_1)$とを結合させればよい．具体的には，偏光分離の後で偏光を水平にしてから1光子干渉が生じるように通常のビームスプリッタで二つの光経路を重ね合わせればよい．光子検出器D_1，D_2，D_3，D_4における光子検出はそれぞれ四つのベル状態のそれぞれへの射影に直接対応している．

最後に，アリスはどの検出器で光子が検出されたのかをボブに知らせる．この情報に基づいてボブは以下のような手順によって偏光状態$|\Psi\rangle$を再生できる．まず，光子2の運動量（経路a_2かb_2）についての重ね合わせ状態を偏光

[6] M.Zukowski は空間についての自由度と偏光自由度の両方を用いることで，元々は3粒子の偏光自由度に対して定義されていたGHZエンタングルメントを2粒子系に対して実現できることを示している．

についての重ね合わせに変換するために，どちらかの経路において90度の偏光回転を行ってから偏光分離素子によって二つの経路を重ね合わせる．続いてアリスから知らされた古典情報に従って，H 偏光と V 偏光とを入れ換えるか否か，二つの偏光成分の間の位相差を π だけシフトするか否かを選択することにより，最終的に光子2の偏光状態を光子1の初期状態に変換することができる．その際にボブは二つの光学素子を操作するだけで十分である．こうして量子テレポーテーションが完了する．

光子を二つしか使わない上に，完全なベル状態測定が可能なこの優れた実験方法によって，量子テレポーテーションが二つの基本的な要素から成立していることが明瞭に示された．すなわち，この実験によって量子情報が古典的な部分と真に量子的な部分とから構成されていること，そして非局所的な量子通信路を介して量子ビットが移されたことが実証された．さらに3.8節で解説した3光子を用いる方法と比べて高い効率をもっている．

しかしながら，この方法では3番めの粒子の量子状態を転送することは明らかに不可能であり，第三者Pによるアリスの光子への初期偏光状態の符号化の作業が不可欠である．さらにまた，状態 Ψ は光子の純粋状態に限定されており，他の系とエンタングルした状態に準備することはできない．実験系の詳細と実験結果については参考文献[78]を参照してほしい．

謝辞：本節の執筆にあたりS.Popescu博士の協力に感謝する．

3.9 連続物理量に対する量子テレポーテーション

(*D.Bouwmeester*)

3.9.1 位置と運動量についてのエンタングルメント

本節では，これまでに説明した方法とはまったく異なる量子テレポーテーションのための量子光学的な方法について解説しよう．この方法は L.Vaidman[79] により提案され，Braunstein と Kimble による発展を経て [80]，その後カリフォルニア工科大学において実証 [81] されたものである．この方法では，偏光についてのエンタングルメントの代わりに位置と運動量との間にあるエンタングルメントを利用しており，量子系の位置と運動量（これらの量は一般に物理系の運動状態を記述している）が離れた場所にある別の量子系の上に移される．この点で，3.7 節や 3.8 節で説明したような系の内部状態である偏光状態が移される方法とは質的に異なるものである．特に，量子系の状態を固有状態の直交基底系を用いて記述しようとすると，位置と運動量についてのエンタングルメントと，偏光についてのエンタングルメントとの間にある質的な違いに気がつく．前者では無限個の固有状態が必要になる．なぜならば，異なる二つの位置（または運動量）の固有値に対応している異なる二つの量子状態の間に直交性を保証するためには，それらの量子状態が無限次元のヒルベルト空間で定義されていなければならないからである．これは光子の偏光状態が二つの直交基底状態の重ね合わせによって完全に表現されるのとは対照的である（偏光は 2 次元のヒルベルト空間で定義される）．

アリスは位置 x_1 と運動量 p_1 で特徴づけられる量子力学的な粒子をもっているとしよう（図 3.18 を参照）．そして，アリスはこの粒子の量子状態を離れた場所にいるボブに送りたいものとしよう．ただし，ハイゼンベルグの不確定性原理によると x の演算子と p の演算子との間には交換関係 $[\hat{x}, \hat{p}] = i\hbar$ が成り立つため，アリスは任意の測定精度で x_1 と p_1 のそれぞれを同時に決定することができないことに注意しなければならない．つまりアリスは自分が送ろうとしている量子状態についての十分な情報を得ることを，量子力学によって禁止されてしまっているのである．この困難を解決する方法は，すでに 3.3 節において考察した方法と概念的には同じものである．

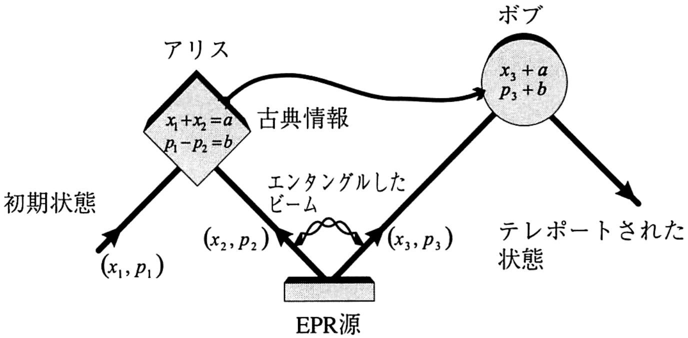


図 3.18　連続物理量の量子テレポーテーションの概念図

図 3.18 に示すように，何らかの EPR 源によってエンタングルした粒子系を生成し，各々の粒子をあらかじめアリスとボブに配っておけばよい．しかしながら，これらの粒子が互いに位置と運動量についてエンタングルしていればよいというわけではない．ここでまず粒子 2 と粒子 3 の間のエンタングルメントとして次のような場合を考えよう．

$$x_2 + x_3 = 0, \qquad p_2 - p_3 = 0 \tag{3.29}$$

各々の粒子の物理量である x_2，x_3，p_2，p_3 の値は式 (3.29) からはまったく定まらない．しかしながら，$x_2 + x_3$ の値と $p_2 - p_3$ の値は確定することに注意しよう．各々の粒子に対しては演算子 x と p は交換しないが，演算子 $x_2 + x_3$ と演算子 $p_2 - p_3$ は交換する．これは結合の符号が位置と運動量とで異なっていることの帰結である．したがって，ここで想定したエンタングル状態では，位置の和 $x_2 + x_3$ と運動量の差 $p_2 - p_3$ は任意の精度で同時に測定することが可能になっている．

次の段階では，アリスは粒子 1 と粒子 2 とに対してベル状態測定と等価な測定を行う．つまり粒子 1 と粒子 2 がエンタングル状態に射影される．光子の偏光状態（内部状態）に対して量子テレポーテーションを行う場合には，ベル状態測定の結果は 4 通りしかありえなかった．これはそれぞれの光子が 2 次元のヒルベルト空間で定義されており，2 光子がエンタングルした状態は 4 次元のヒルベルト空間で定義されるためである．しかし，ここではアリスは

連続的な値をもつ二つの物理量

$$x_1 + x_2 = a\,, \qquad p_1 - p_2 = b \tag{3.30}$$

を測定することになる．ここで a と b は連続的な値域をもつ実数である．このことは，二つの粒子についての位置の和と運動量の差を測定するためには無限（大）次元のヒルベルト空間における射影が必要になることを示唆している．

式 (3.29) で与えられた初期エンタングルメントとアリスによる測定 (3.30) の結果，ボブのところにある粒子 3 の状態は

$$x_3 = x_1 - a\,, \qquad p_3 = p_1 - b \tag{3.31}$$

で表されることになる．

最後にアリスが測定結果 a と b を知らせれば，ボブは粒子 3 の位置と運動量をそれぞれ a，b だけ補正することにより粒子 1 の初期量子状態を粒子 3 の上に再生できる．

3.9.2 量子光学的な方法による実験

連続量の量子テレポーテーションの実験はカリフォルニア工科大学のグループによってはじめて行われた [81]．この実験では，粒子の位置と運動量を直接扱う代わりに，演算子 (x, p) と同様な交換関係に従う二つの物理量によって特徴づけられる特殊な（非古典的な）光波を用いている．量子化された単一モードの光の場は量子力学的な調和振動子によって記述できるので，このような置き換えが可能になるのだ［106-109］．

質点の質量 m，周波数 ω，変位 x，運動量 p の古典的な調和振動子の運動はハミルトニアン

$$H = \frac{p^2}{2m} + \frac{m}{2}\omega^2 x^2 \tag{3.32}$$

によって記述される．量子力学的なハミルトニアンを得るには，x と p を交換関係 $[\hat{x}, \hat{p}] = i\hbar$ に従う演算子 $(x \to \hat{x},\ p \to \hat{p} = i\hbar\partial/\partial x)$ に置き換えればよい．ここで

$$\hat{x} = \sqrt{\frac{\hbar}{2m\omega}}\left(\hat{a}^\dagger + \hat{a}\right) \tag{3.33}$$

$$\hat{p} = i\sqrt{\frac{\hbar m\omega}{2}}\left(\hat{a}^\dagger - \hat{a}\right) \tag{3.34}$$

を定義しよう．すると量子化された調和振動子のハミルトニアンは自然な形

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) \tag{3.35}$$

になる．演算子 $\hat{a}$ と $\hat{a}^\dagger$ は以下のような関係式によって特徴づけられる．

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle\,, \qquad \hat{a}|0\rangle = 0 \tag{3.36}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{3.37}$$

$$\left[\hat{a}\,,\hat{a}^\dagger\right] = 1\,, \qquad [\hat{a}\,,\hat{a}] = \left[\hat{a}^\dagger\,,\hat{a}^\dagger\right] = 0 \tag{3.38}$$

$$\hat{a}^\dagger\hat{a} = \hat{N} \tag{3.39}$$

ここで $|n\rangle$ は量子力学的な調和振動子の n 番めの励起状態であり，$\hat{N}$ は励起の数の演算子である．式 (3.36) と (3.37) によれば，演算子 $\hat{a}$ と $\hat{a}^\dagger$ はそれぞれ調和振動子の消滅（下降）演算子と生成（上昇）演算子である．

周波数 ω をもつ単一モードの量子化された光の場は演算子 $\hat{a}$ と $\hat{a}^\dagger$ によって表現される．一定の振幅 E_0 と単一の偏光モードを想定した最も基本的な表現では，ある位置における電場ベクトルの演算子は

$$\hat{\bar{E}}(t) = E_0\left(\hat{a}e^{-i\omega t} - \hat{a}^\dagger e^{+i\omega t}\right) \tag{3.40}$$

で与えられる．ここで演算子 $\hat{a}^\dagger$ と $\hat{a}$ はそれぞれ光子の生成演算子と消滅演算子となっている．調和振動子との類推から次のような演算子 $\hat{X}$ と $\hat{P}$ を新たに導入しよう．

$$\hat{X} = \left(\hat{a}^\dagger + \hat{a}\right) \tag{3.41}$$

$$\hat{P} = i\left(\hat{a}^\dagger - \hat{a}\right) \tag{3.42}$$

すると電場の演算子は，演算子 $\hat{X}$ と $\hat{P}$ を用いて以下のように表すことができる．

$$\hat{\bar{E}}(t) = E_0\left(\hat{X}\cos(\omega t) + \hat{P}\sin(\omega t)\right) \tag{3.43}$$

演算子 $\hat{X}$ と $\hat{P}$ の固有値は直交位相振幅と呼ばれ，それぞれ電場のイン・フェーズな成分，アウト・オブ・フェーズな成分として解釈されている．交換関係 $[\hat{X},\hat{P}] = 2i$ から，関係式 $\Delta X\Delta P = 1(\langle\Delta A\rangle^2 = \langle A^2\rangle - \langle A\rangle^2)$ が導かれる．この関係式はイン・フェーズな成分とアウト・オブ・フェーズな成分と

を任意の精度で同時に測定することは不可能であることを意味しており，量子力学的な粒子における位置 X と運動量 P との間の不確定性関係に類似している．このようにして粒子の位置 X と運動量 P を，単一モードの光の場における X 成分と P 成分とに対応づけることができる．

連続量の量子テレポーテーションを実現するための次の段階は，互いにエンタングルした二つの特殊な（非古典的な）光波の場を作ることである．そのためにはまず，スクィーズド光の概念について説明しなければならない [108]．ここで図 3.19 に示すように，単一モードの光の場の状態を平面 (X,P) で記述することにしよう．真空状態は原点を囲む円盤 1 によって表され，コヒーレント状態は円盤 2 によって記述される．ここで後者は真空状態が変位したものとみなすことができる．円盤の拡がりは X と P の値における最小不確定性を示している．不確定性による拡がりは X と P とで同じであるが，関係式 $\Delta X \Delta P = 1$ を満たすためには必ずしも両者の拡がりが同じである必要はない．図 3.19 に示した楕円はそのような状態（スクィーズド状態）であり，P 方向に縮む $((\Delta P)^2 > 1)$ とともに X 方向には拡がっている $((\Delta X)^2 > 1)$．

ここで，それぞれ X と P について最大にスクィーズされた二つの特殊な

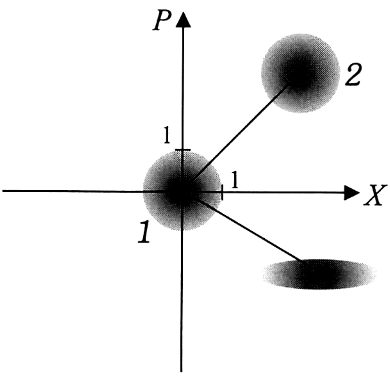


図 3.19 単一モードの光波の場の量子状態を $X-P$ 平面で表したもの：X はイン・フェーズな振幅成分，P はアウト・オブ・フェーズな振幅成分を表している．原点を囲む円領域 1 は最小不確定関係を満たす真空状態である．円領域 2 はコヒーレント状態であり，真空状態から変位した状態として理解される．楕円形の領域はスクィーズド状態を表している（P 方向にスクィーズされている）

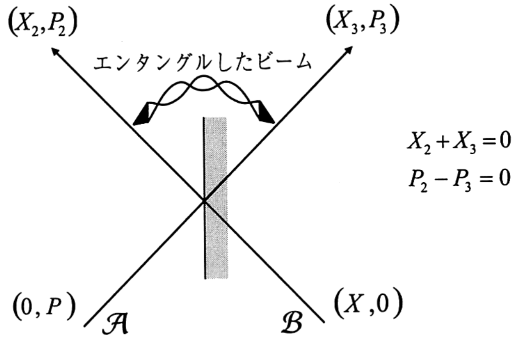


図 3.20　互いにエンタングルした二つの光波の場を作り出す方法．それぞれ X 方向および P 方向について最大にスクィーズされた二つの光波 A と B を分岐比 1:1 のビームスプリッタの各ポートから入力すると，異なる出力ポートから出てくる二つの光波はエンタングルしている

光波の場 A と B を考えよう．そして図 3.20 に示すように，等分岐比をもつビームスプリッタの二つの入力ポートから，それぞれ光波の場 A と B を入力しよう．するとビームスプリッタの後における光波の場 2 と 3 は次のように関係づけられることになる．

$$X_2 + X_3 = 0\ , \qquad P_2 - P_3 = 0 \tag{3.44}$$

これこそまさに必要としていたエンタングル状態にほかならない [81]（偏光についてエンタングルした光波の場については参考文献 [110]–[112] を参照のこと）．

スクィーズド光を発生するには，非線形光学結晶中でのパラメトリック増幅過程 [107, 112, 113] を利用すればよい．周波数 ω_1 の入力信号光と周波数 ω_3 の強いポンプ光とが非線形光学結晶中で相互作用することにより周波数 $\omega_2 = \omega_3 - \omega_1$ をもつ第 3 の光波が新たに発生する（図 3.21 参照）．以下では最も簡単な場合，すなわち偏光モードは一つ，三つの光波の進行方向は同じで位相整合条件は満たされており，さらに $\omega_1 = \omega_2 = \omega$，$\omega_3 = 2\omega$ を想定する．

周波数 ω の光波の状態は，非線形光学結晶中で周波数 2ω の強い光と相互

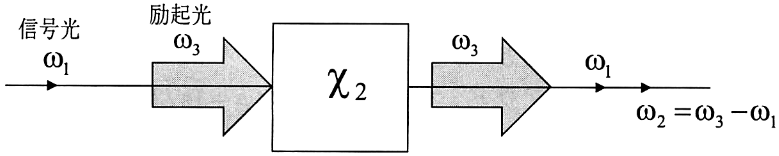


図 3.21 パラメトリック光増幅：周波数 ω_1 をもつ入力信号光は非線形光学結晶（χ_2 媒質）中で周波数 ω_3 をもつ強度の強いポンプ光と相互作用する．非線形相互作用の結果，入力信号光は増幅され，かつ周波数 $\omega_2 = \omega_3 - \omega_1$ をもつ第 3 の光が発生する

作用することにより，以下のハミルトニアンに従って時間発展する．

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) + S\cos(2\omega t)\left(\hat{a}^\dagger - \hat{a}\right)^2 \tag{3.45}$$

ここで右辺の第 2 項が古典的な光として近似された強いポンプ光との相互作用を表している．S は結晶の非線形性の強さとポンプ光の強度で決まる係数である．エネルギー保存の法則を利用すると第 2 項は

$$S\left((\hat{a})^2 e^{i2\omega t} - (\hat{a}^\dagger)^2 e^{-i2\omega t}\right) \tag{3.46}$$

に書き換えられる．ハイゼンベルグ描像に基づいて電場の演算子の時間発展を調べるためには，演算子 $\hat{a}$ と $\hat{a}^\dagger$ がそれぞれ

$$\frac{d\hat{a}}{dt} = -\frac{i}{\hbar}\left[\hat{a}\,,\hat{H}\right] = -i\omega\hat{a} - iS\hat{a}^\dagger e^{-i2\omega t} \tag{3.47}$$

$$\frac{d\hat{a}^\dagger}{dt} = -\frac{i}{\hbar}\left[\hat{a}^\dagger\,,\hat{H}\right] = i\omega\hat{a}^\dagger + iS\hat{a}e^{+i2\omega t} \tag{3.48}$$

に従って時間発展することを利用すればよい．ここで，式 (3.41) と (3.42) で定義された演算子 $\hat{X}$ と $\hat{P}$ を用いて変換すると，直交位相振幅成分の時間発展についての簡単な方程式

$$\frac{d\hat{X}}{dt} = S\hat{X}\,, \qquad \frac{d\hat{P}}{dt} = -S\hat{P} \tag{3.49}$$

を得ることができる．それらの解は

$$\hat{X}(t) = \hat{X}(0)e^{St}\,, \qquad \hat{P}(t) = \hat{P}(0)e^{-St} \tag{3.50}$$

である．相互作用時間 t の関数としてイン・フェーズな成分の振幅 $\hat{X}$ は指数関数的に増大し，他方でアウト・オブ・フェーズな成分の振幅 $\hat{P}$ は指数関数

的に減少することがわかる．このように周波数縮退したパラメトリック増幅過程は位相に敏感な増幅器として機能する（イン・フェーズ ($\varphi = 0 \mathrm{mod}\pi$) である入力信号を増幅し，アウト・オブ・フェース ($\varphi = (\pi/2) \mathrm{mod}\pi$) である成分を減衰させる）．言い換えると，入力信号光に対するパラメトリック増幅は光の場の P 成分をスクィーズすることになる．

相互作用時間を長くしてスクィージングの度合を強めるために，非線形光学結晶は周波数 ω に共振した光共振器の内部に配置されることが多い．このような系は光パラメトリック発振器 (OPO: Optical Parametric Oscillator) と呼ばれており，レーザ発振を避けるために共振器損失はわずかにパラメトリック増幅利得より高めに設定されていて，高強度の光の立ち上がりは結晶中での飽和効果（高次の非線形効果）を引き起こすことになる．参考文献 [81] の実験では，光パラメトリック発振器への外部信号光の入力はなく，真空状態から増幅した光を用いている．

以上見てきたように，二つのスクィーズド光とビームスプリッタを用いると，互いにエンタングルした二つの特殊な光波を作り出すことができる．そこで，次はどのようにしてベル状態測定を行うのかを説明しよう．3.5 節で議論した偏光エンタングル状態に対するベル状態測定器と比べると，これから説明するエンタングル状態への射影測定ははるかに直接的である．(X_1, P_1) で特徴づけられた光波 1 と (X_2, P_2) で特徴づけられた EPR 源からの出力光の片割れ（光波 2）とを等分岐比のビームスプリッタの上で重ね合わせれば，それぞれの出力ポートから出てくる二つの光波の状態は

$$(X_{\mathcal{C}}, P_{\mathcal{C}}) = (X_1 - X_2, P_1 - P_2), \quad (X_{\mathcal{D}}, P_{\mathcal{D}}) = (X_1 + X_2, P_1 + P_2) \tag{3.51}$$

によって特徴づけられることになる．そこで平衡型ホモダイン光検出（参考文献 [107] を参照）を行えば，アリスは光波 D に対して X 成分を測定し，光波 C に対して P 成分を測定することができる．これらはそれぞれ $a = X_1 + X_2$, $b = P_1 - P_2$ に対応しているので，量子テレポーテーションが可能になる．平衡型ホモダイン光検出を行うためには，まず等分岐比のビームスプリッタ上で信号光の場と局発光とを重ね合わせて，次にそれぞれビームスプリッタの二つの出力ポートのそれぞれに設置された検出器における光電流（光の電場の強度に比例）の強度差を記録する．測定された強度差は局発光の位相 φ の

関数として

$$I(\varphi) = C\,(X \sin\varphi + P \cos\varphi) \tag{3.52}$$

により与えられる [107]．ここで C は局発光の強さと検出器の効率に依存した定数である．局発光の位相 φ を調整することにより，二つの直交位相振幅成分 X と Y についての任意の重ね合わせ状態を測定できることに注意しよう．

量子テレポーテーションの一般的な手順に従い，アリスは a と b の測定結果をボブに知らせ，それをもとにボブは光の場の状態を補正する．ボブが実際にこの操作を行うためには，エンタングルした光波の片割れである光波 3 を反射率 99%の半透過鏡により反射させて，その際に a と b の値に応じて振幅と位相を変調した光を反対側のポートから入力して重畳させればよい．このようにしてボブは，少なくとも原理的には，はじめにアリスの手元にあった光波の量子状態をほとんど完全に自分の手元に再生することができる．

実際の実験では参考文献 [81] に見られるように，強くスクィーズされた光波を発生したり光波の位置や位相の微調整のためにいくつかの高度な技術が必要になる．アリスの手元にあった初期状態とボブの元へ転送された量子状態との間の重なりの程度を測定して，量子テレポーテーションの忠実度を評価すると，実験における技術的な不完全性のために現状では 0.58 ± 0.02 に制限されてしまっている．とはいうものの，この値はアリスとボブの間での古典的な通信のみによって達成可能な値（ただし，出力された光の状態はコヒーレント状態になるという前提をおく）である 0.5 を明らかに上回っている．

謝辞：本節への有益なコメントに対して H.J.Kimble 博士と E.S.Polzik 博士に感謝する．

3.10　エンタングルメント・スワッピング：エンタングルメントに対する量子テレポーテーション

(*D. Bouwmeester, J-W. Pan, H. Weinfurter, A. Zeilinger*)

エンタングルした二つの粒子を準備するには，そのような状態を出力する粒子源を直接利用するか [94, 114]（3.4 節参照），あるいは二つの独立な粒子を相互作用させて作ればよい [103, 115]（4.3 節，5.2.4 項および 5.2.11 項にて後述）．これらとは異なる第三の方法として，二つの独立な粒子の状態をエンタングル状態の一つに射影することでも 2 粒子エンタングルメント状態を得ることができる．このような射影測定によるエンタングルメント生成では，エンタングルさせたい二つの粒子の間に必ずしも直接の相互作用がある必要はない．もし二つの粒子のそれぞれがあらかじめそれぞれ別の粒子を相手方としてエンタングルしていたような場合には，これらの相手方となる二つの粒子に対してベル状態測定などの適切な測定を行うことにより，はじめの二つの粒子の間に自動的にエンタングルメントが形成されることになる．これは射影定理の直接の応用であり，エンタングルメント・スワッピングと呼ばれている [74, 85, 87]．

図 3.22 に示すように，二つの独立な EPR 源からエンタングルした粒子対が同時に出力されるものとしよう．これらの粒子対のそれぞれは偏光エンタングルメント状態 $|\Psi^-\rangle$ であり，全系の状態は

$$|\Psi\rangle_{1234} = \frac{1}{2}\left(|\mathrm{H}\rangle_1 |\mathrm{V}\rangle_2 - |\mathrm{V}\rangle_1 |\mathrm{H}\rangle_2\right)\left(|\mathrm{H}\rangle_3 |\mathrm{V}\rangle_4 - |\mathrm{V}\rangle_3 |\mathrm{H}\rangle_4\right) \tag{3.53}$$

で表されるとしよう．ここで光子 1 と光子 2 は第 1 の対に属しており，光子 3 と光子 4 は第 2 の対に属している．異なる対に属する二つの光子の間にはエンタングルメントは存在していない．

次に光子 2 と光子 3 に対してベル状態測定を行って，3.5 節で説明したようにこれら 2 光子の直積状態を四つのベル状態の中のどれか一つの状態に射影することにしよう．この測定の結果，光子 1 と光子 4 の状態もまたベル状態のどれか一つに射影されることになる．どのベル状態に射影されるかは光子 2 と光子 3 に対するベル状態測定の結果に依存している．全系の初期状態が

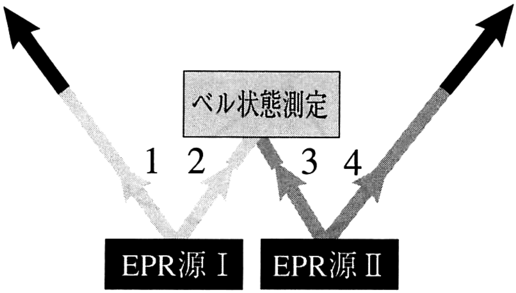


図 3.22 エンタングルメント・スワッピングの原理：二つの EPR 粒子源はそれぞれエンタングルした光子対である光子 1–光子 2 と光子 3–光子 4 を作り出す．それぞれの光子対からそれぞれ一つずつ光子を取りだして（光子 2 と光子 3）ベル状態測定を行う．その結果，光子 1 と光子 4 は互いにエンタングルした状態に射影される．右側の矢印の色の変化は取りうる四つの状態のうちのどれか一つに射影されたことを意味している

式 (3.53) で記述される場合，光子 1 と光子 4 についてのベル状態は，まさに光子 2 と光子 3 が射影されたベル状態と同じになる．このことは式 (3.53) が

$$|\Psi\rangle_{1234} = \frac{1}{2}\Big(\left|\Psi^+\right\rangle_{14}\left|\Psi^+\right\rangle_{23} - \left|\Psi^-\right\rangle_{14}\left|\Psi^-\right\rangle_{23} - \left|\Phi^+\right\rangle_{14}\left|\Phi^+\right\rangle_{23} + \left|\Phi^-\right\rangle_{14}\left|\Phi^-\right\rangle_{23} \Big) \tag{3.54}$$

のように書き換えられることから明白である．こうして直接相互作用をしていないにもかかわらず光子 1 と光子 4 の間にエンタングルメントが形成された．そして光子 2 と光子 3 に対する射影測定の結果から，光子 1 と光子 4 との間のエンタングルメントについても知ることができる．

すでに 3.7.2 項でふれたように，エンタングルメント・スワッピングはエンタングル状態に対する量子テレポーテーションとみなすこともできる．実際に図 3.23 に示したエンタングルメント・スワッピングの実験系の構成は，図 3.12 で説明した量子テレポーテーションの実験系に酷似している．これらの実験系に共通な基本構成は 3.7 節において説明済みである．二つの実験の間の相違点は，単一光子の量子ビットの量子テレポーテーションの実験（図 3.12）では光子 4 は光子 1 の存在を示すトリガーとして用いられていたのに対し，エンタングルメント・スワッピングの実験（図 3.23）では二つの光子対のそれぞれにおける偏光エンタングルメントがともに有効に活用されている．

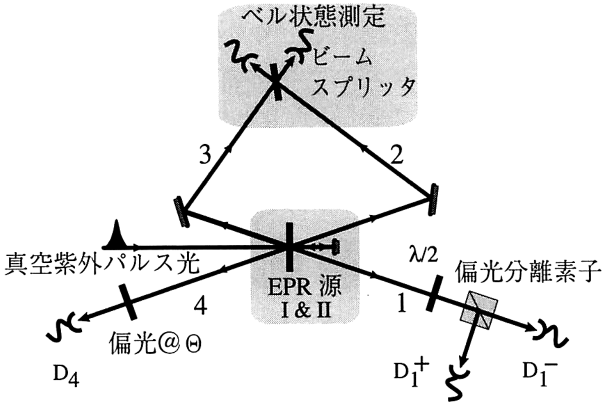


図 3.23　エンタングルメント・スワッピングの実験系：真空紫外のポンプパルス光は非線形結晶を通過する際にエンタングルしている光子の対（光子 1–光子 2）を生成する．その後，光子 2 はビームスプリッタに導かれる．一方でポンプパルス光は反射されて結晶中を逆行するときに第 2 の光子対（光子 3–光子 4）を生成する．その後，光子 3 もまたビームスプリッタへ導かれる．光子 2 と光子 3 はビームスプリッタで重ね合わされて，その二つの光子検出器により同時計数される．その結果，光子 2 と光子 3 の状態は $|\Psi^t\rangle_{23}$ に射影される．このベル状態測定の結果，光子 1 と光子 4 の状態もまたエンタングル状態に射影される．このエンタングルメントを解析するために，偏光角を変化させて検出器 D_1^+ と D_4 との間の相関，および検出器 D_1^- と D_4 との間の相関を調べる．偏光分離素子の前の半波長板を回転することにより光子 1 に対してあらゆる偏光基底を選択することができる．検出器 D_1^+ と D_4 における同時計数，そして検出器 D_1^- と D_4 における同時計数は，ベル状態 $|\Psi^t\rangle_{23}$ が得られたときにのみ意味をもっているので，実際には四つの検出器における同時計数を見ていることになる

エンタングルメント・スワッピングは，光子 2 の状態を光子 4 へ，あるいは光子 3 の状態を光子 1 へと量子テレポーテーションにより移しているとみなすこともできる．これらはまったく等価である．ここで注目すべきは，転送された光子の状態それ自体は単一の光子状態としては定義できないという点である．よく知られているように，他の粒子と最大限にエンタングルした粒子の状態は純粋状態ではなく，最大限に混合した密度行列によって説明されなければならない．したがって，このような状況において量子テレポーテー

ションの対象とされたのは，光子の量子状態それ自体ではなく，その光子がもう一つの光子とエンタングルしているその在り様なのである．

エンタンングルメント・スワッピングの手順に従えば，光子 2 と光子 3 とがベル状態 $|\Psi^-\rangle_{23}$ に射影された場合には，光子 1 と光子 4 もまたベル状態 $|\Psi^-\rangle_{14}$ に射影されることになる．実際にこのことを確認するためには，光子 1 と光子 4 との間の偏光相関を解析しなければならない．このとき，ベル状態測定器の二つの光子検出器との間で 4 光子の同時計数を行うことになる．もし光子 1 と光子 4 が状態 $|\Psi^-\rangle_{14}$ にあるのであれば，偏光基底のとり方にはよらずそれらの光子の偏光は互いに直交していなければならないはずである．22.5 度の方向に設定した半波長板と偏光分離素子の後においた二つの光子検出器（D_1^+ と D_1^-）を用いて，光子 1 に対して；45 度直線偏光 (D_1^+) と −45 度直線偏光 (D_1^-) の状態を解析する．一方で光子 4 は任意の方向 Θ に偏光方向を向けられてから検出器 D_4 において検出される．

エンタングルメント・スワッピングが起こっているのであれば（ベル状態測定結果 $|\Psi^-\rangle_{23}$ で条件づけされた）D_1^+ と D_4 間での同時計数と D_1^- と D_4 間での同時計数は Θ の関数としてそれぞれ互いに 90 度だけずれた sin 曲線を描くはずである．$\Theta = 45$ のときに $D_1^+D_4$ の値 0 になり $D_1^-D_4$ の値は最大となる．それらの実験結果を図 3.24 に示す（図 3.24 はいうまでもなくベル状態測定器の二つの検出器の両方で光子が検出されたという条件のもとで抽出されたものである）．

この方法では四つの光子の同時計数が必要である．実験結果は予想どおりに D_1^+ と D_1^- との間で相補的な sin 曲線を示している．さらに半波長板の回転角を変えて光子 1 に対する偏光基底のとり方を変更しても，やはり同様な sin 曲線が得られることを確認した．測定で得られた可視度の値 0.65 は，古典波動理論から導出される上限値 0.5 を明らかに上回っている．ここで示した実験結果は明らかに量子力学的な状況において量子テレポーテーションを実現したものであるといえるだろう．なぜならば，二つの粒子は元はといえば独立に発生したものであり過去に一度たりとも直接に相互作用したことはなく，それにもかかわらずこれらの粒子の間にエンタングルメントが形成されたのは，まさにエンタングルメント・スワッピングの結果だからである．次節ではエンタングルメント・スワッピングのいくつかの利用方法を紹介しよう．

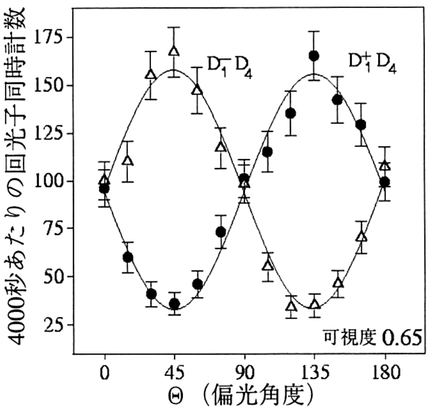


図 3.24　エンタングルメントの検証：偏光角 Θ の変化に対する同時計数 $D_1^+D_4$ と $D_1^-D_4$ の変動（状態 $|\Psi^t\rangle_{23}$ が得られたという条件のもとで）．図中の二つの相補的な sin 曲線は光子 1 と光子 4 との間には偏光のエンタングルメントがあることを示している

3.11　エンタングルメント・スワッピングの応用

(*S. Bose, V. Vedral and P.L. Knight*)

エンタングルメント・スワッピングにはいくつかの利用方法がある．ここでは量子交換処理，2 者間でのエンタングルメント配布の高速化（逐次的なエンタングルメント精製），そして多粒子間エンタングルメント生成について紹介しよう．

3.11.1　量子交換処理

ネットワークに N 人のユーザがつながっているものとしよう．まず各ユーザは中央交換機との間でそれぞれベル状態にある二つの粒子のそれぞれを分け合っているとする．図 3.25 に示したように，ユーザ A，B，C，D は中央交換機 O との間で，それぞれベル状態粒子対 (1,2)，(3,4)，(5,6)，(7,8) を分け合っている．ここでユーザ A，B，C が 3 粒子の GHZ 状態を分け合うことを望んでいるとしよう．そこで中央交換機において粒子 2，粒子 3，粒子 5 を

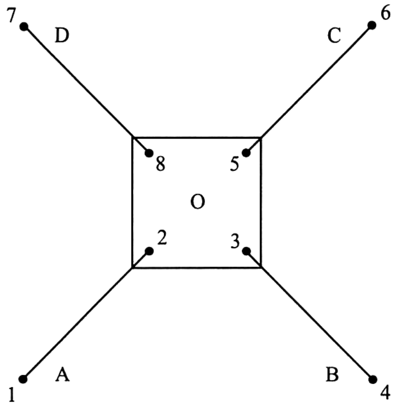


図 3.25 エンタングルメント配布の概念図．最初にユーザ A，B，C，D は，それぞれ中央交換機との間でベル状態対を分け合っている．交換機で適切な結合測定を行うだけで，A，B，C，D の何人かの間でエンタングルメントを分け合うことができる

GHZ 状態に射影する測定を行う．すると，それぞれユーザ A，B，C の手元にある粒子 1，粒子 4，粒子 6 の状態は GHZ 状態に射影されることになる．同様にして，N 人のユーザの間で N 粒子のシュレーディンガーの猫状態を生成することができる．

N 粒子のエンタングルメントを直接生成してからそれぞれのユーザに配送するのと比べて，このような量子交換処理の方法には次のような利点がある．

(A) 各ユーザは，中央交換機との間で分け合っている部分的にデコヒーレンスを受けてしまった数多くの不完全ベル状態の対から，エンタングルメント精製によって少数のしかし完全なベル状態粒子対を取り出すことができる．これは複数のユーザの手元にある多粒子の間にシュレーディンガーの猫状態を作り出す出発点となるものである．また粒子を配送するときに生じてしまうデコヒーレンスの問題を少なくとも原理的には回避することができる．さらに付け加えると，N 粒子のシュレーディンガーの猫状態に対する多地点間エンタングルメント精製を回避できる．なぜならば，はじめに 2 粒子のエンタングルメントを精製しておけば，後は量子交換処理の手順で純度の高い多粒子状態に到達できるからである．

(B) 必要なときに必要な数の粒子を必要な仕方でエンタングルさせること

ができる．最初はどのメンバーが N 粒子のエンタングルメントを必要とするのかわかっていないかもしれない．そこで将来生じうるありとあらゆる要望に応えられるように初期状態を準備しておかなければならないだろう．しかし，これではあまりに非経済的ではある．一方で，もし必要に応じて必要なユーザだけの間で N 粒子のエンタングル状態を作り出すことができればはるかに便利であろう．

Biham, Huttner, Mor らは時間反転された EPR の方法によって接続と交換を行うことを特徴とする暗号ネットワークについての同様な方法を提案している [116].

3.11.2　エンタングルメント配布における所要時間の短縮

ベル状態にある原子系または電子の系（質量のある粒子の系全般）の部分系を離れた 2 者の各々に配布しようとする場合，標準的なエンタングルメント・スワッピングを利用することで処理時間が短縮されうることを示す．種明かしは両者の間にいくつものベル状態粒子対の発生装置とベル状態測定器とを設置することである．図 3.26(a) に見るように，二人のユーザ A と B の間は距離 L だけ隔たっていて，中間地点 O にはベル状態粒子対の発生装置が置いてある．A と B のそれぞれに粒子が到達するには少なくとも $t = L/2v$ ($v < c$（真空中の光速度））だけの時間を必要とする．次に図 3.26(b) に見るように，A と O の中間地点および B と O の中間地点にそれぞれ中継点 C と D を設置する．ここで中間地点 O にはベル状態測定器だけが置かれることになる．時刻 $t = 0$ に，中継点 C および D はそれぞれベル状態粒子対 (1,2) および (3,4) を送り出す．粒子 2 と粒子 3 は中間地点 O に到着し，粒子 1 と粒子 4 はそれぞれユーザ A および B の手元に届く．それらの伝播に要する時間は $t = L/4v$ である．そして，この瞬間に中間地点 O において粒子 2 と粒子 3 に対してベル状態測定を行う．この測定に伴い，それぞれ A および B にある粒子 1 と粒子 4 の状態がベル状態に射影される．測定に要する時間を t_m とすると，A と B の間にベル状態粒子対を供給するのに必要な時間は（C と D を中継点とした場合）$t_2 = L/4v + t_m$ となる．$t_m < L/4v$ である限り時間 t_2 は t_1 より短い．もちろん，中間地点 O から A と B にベル状態測定の結果を知らせるのに要する時間も考慮しなくてはならない．光子のベル状態粒子対を配布する場合には，この方法を採用したところで処理時間が節約されると

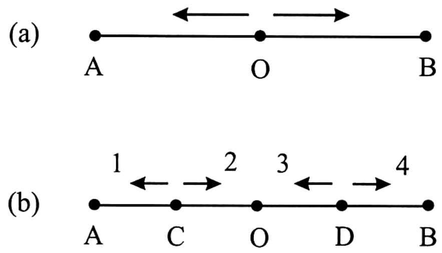


図 3.26 二人の離れたユーザ A と B の間で，エンタングルした（有限質量の）粒子の対のそれぞれを分かち合うために必要な時間を短縮するための方法．中継点 C と D を設けてそれぞれベル状態対を発生させ，そして中間点 O でベル状態測定を行う．このようにして，粒子の移動に要する時間を短縮できる

いうことにはならない．しかしエンタングルしている粒子が質量をもっている場合には，この方法によって配布に要する時間を短縮することができるだろう．このようにして，途中で利用するベル状態対の数が多ければ多いほど離れた 2 者間でベル状態粒子対を共有するのに必要な時間は短縮される．

3.11.3 粒子の伝播中に生じたエンタングルメントの劣化に対する誤り訂正

伝播中に生じたエンタングルメントの劣化を補正するために，エンタングルメント・スワッピングが利用できることを示そう（ただし，この処理は後述するように確率的な性質をもつ）．図 3.26(b) において中継点 C および D から送り出されたベル状態粒子対は，伝播の途中で確率振幅のエラーのためにエンタングルメントが劣化した状態

$$|\Psi\rangle = \cos\theta|01\rangle + \sin\theta|10\rangle \tag{3.55}$$

に変ってしまうと想定しよう．そのため粒子 2 と 3 が中間地点 O に到着した時点では，2 個のエンタングルした粒子対の全系の量子状態は

$$\begin{aligned}|\Phi\rangle &= \cos^2\theta|0101\rangle + \sin\theta\cos\theta(|1001\rangle \\ &+ |0110\rangle) + \sin^2\theta|1010\rangle\end{aligned} \tag{3.56}$$

で与えられることになる．粒子 2 と 3 に対してベル状態測定が行われたとき，ベル状態 $|00\rangle+|11\rangle$ またはベル状態 $|00\rangle-|11\rangle$ に見いだされる確率は $\sin^2 2\theta/2$ であり，他の二つのベル状態に見いだされる確率は $(1+\cos^2 2\theta)/2$ となる．前

者の場合には粒子1と粒子4はベル状態 $|00\rangle + |11\rangle$ または $|00\rangle - |11\rangle$ に射影される．このときには，粒子の伝播中に確率振幅のエラーが生じているにもかかわらず，AとBは完全なベル状態粒子対を共有できる．もちろん粒子2と粒子3が他の二つのベル状態に見いだされたときには，粒子1と粒子4の状態は式 (3.55) の状態よりもさらに不完全なエンタングル状態になってしまう．このようにして，確率的という制限はつくもののエンタングルメント・スワッピングを確率振幅に生じた誤りの訂正に利用できる．

この場合，成功確率は $\sin^2 2\theta/2$ であり失敗確率 $(1+\cos^2 2\theta)/2$ よりも小さい．しかしながら，たまたま誤り訂正に成功した場合にはベル状態測定の結果からその成功を知ることができる．これは逐次的なエンタングルメント精製の一種であるとみなせるかもしれない．それとは異なり，標準的なエンタングルメント精製は並列処理である [47, 117]（8.2節で後述）．ここで示したような精製の過程で保存される量——エンタングルメントの測度——の存在を示すことができる [118]（6.4節のエンタングルメントの測度の項を参照）．

3.11.4　より多くの粒子をエンタングルさせるには

エンタングルしている粒子の数が少ない状態から多くの粒子がエンタングルしている状態を，エンタングルメント・スワッピングによって作り出すことができる．その基本になるのはGHZ状態（三つの粒子が最大にエンタングルした状態）とベル状態測定器である．ここではどのようにして N 個の粒子が最大にエンタングルした状態から $N+1$ 個の粒子が最大にエンタングルした状態を生成するのかを考えよう．まず N 個の最大にエンタングルした状態から一つの粒子を取り出し，そしてGHZ状態を形成している別の三つの粒子の中の一つの粒子を取り出して，これら二つの粒子に対してベル状態測定を行う．その結果，これら二つの粒子の状態はベル状態となり，残りの全部で $N+1$ 個の粒子は最大にエンタングルした状態になる．この過程を記号的に表すと

$$|E(N)\rangle \otimes |E(3)\rangle \xrightarrow{\text{ベル状態測定}} |E(N+1)\rangle \otimes |E(2)\rangle$$

となる．図3.27は，4粒子が最大にエンタングルしている状態から5粒子が最大にエンタングルしている状態を作り出す過程を図式的に表したものである．

さてここで「それではGHZ状態はどうやって作るのか」という疑問が生

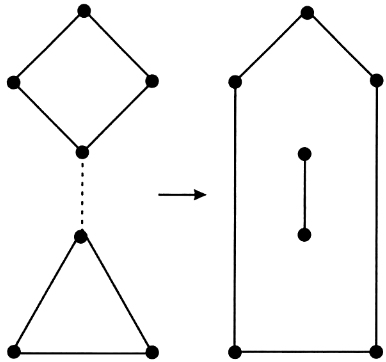


図 3.27 四つの粒子がエンタングルしている状態と GHZ 状態とから，ベル状態測定によって五つの粒子がエンタングルしている状態を作り出す

じる．Zeilinger により示唆された方法はその一つの答えである [119]（三つの光子のエンタングルメントを作る方法については 6.3.4 項を参照のこと）．3 個のベル状態対から出発して，そのそれぞれから光子を一つずつ取り出して GHZ 状態測定を行っても，残りの 3 個の光子の状態は GHZ 状態になる．3 個のエンタングルした粒子対から 3 粒子の GHZ 状態を生成する明瞭な方法は，はじめに Zukowski らによって提案されている [101].

第4章

量子計算の概念

量子計算について解説するにあたりさまざまな方法やレベルがある．本章ではこのことを反映しようと思っている．本章は三つの独立した節から構成されている．4.1 節では基本的な論点を強調しつつも数学的な形式化は避け，主題の最も基本となる事柄について紹介する．多くの人はこのレベルの説明で十分目的を達成できる．詳細を知りたい人は 4.2 節に進むことを勧める．4.2 節では読者に非常に高速な量子アルゴリズムから，計算量の議論を経て，量子素因数分解といったより先端的なトピックスまでを紹介する．最後にいま一つ重要なことを述べるが，4.3 節では難解な理論的アイデアを実際に動作する素子に変換する方法を与える．第 5 章では量子計算の今までの実験成果とさらなる発展のために続けられている努力について述べる．

4.1　量子計算入門

(*D. Deutsch, A. Ekert*)

4.1.1　自然を利用する新しい方法

科学技術の歴史における多くの重大時点で，自然を利用する——物質，力，エネルギー源といったさまざまな物理資源を活用する——新しい方法の発見を伴ってきた．20 世紀には，コンピュータの発明により複雑な情報処理が人間の脳以外で実行できるようになったとき，**情報** (information) がこのリストに加えられた．コンピュータ技術の歴史はそれ自身ある種の物理的具現化か

ら別の物理的具現化 —— ギアからリレー，バルブ，トランジスタ，集積回路など —— への一連の変化を伴っていた．今日の先端的な平板印刷技術は，シリコンチップの表面を横断するミクロンより小さな論理ゲートや配線をエッチングすることができる．まもなくこれらの技術は，ほんの数個の原子で論理ゲートが構成されるほどの大きさになるまで，より小さな部品さえも作り出せるであろう．

人間の知覚かそれより大きな尺度では古典（非量子的）物理法則が現象をうまく近似するが，原子的尺度では量子力学の法則が支配的であり，まったく異なる特性を備えている．もし，コンピュータがより速く（それゆえより小さく）なり続けるのであれば，新たに，**量子**技術が現在のものに置き換わるか補間されなければならないが，そのような技術はより小さくかつより速いマイクロプロセッサよりはるかにすぐれたものを提供することができるであろう．それは，古典に類を見ない新しい量子アルゴリズムにより，まったく新しい計算様式を支持する．また，計算の量子論は物質の枠組みに対し古典的な前任者が演じてきたものよりさらに基本的な役割さえ演じており，物理学か情報処理を基礎から理解しようとする人はその新しい見識を世界観に組み込まなければならない．

4.1.2　ビットから量子ビットへ

量子コンピュータを古典的なものと区別するものは何か？　情報の基本単位，**ビット** (bit) を注意深く見てみよう．ビットと量子ビットについてはすでに第 1 章で説明されているが，ここでの説明を完全かつ矛盾のないものにするため，再度述べることにした．

物理的観点からビットは 2 状態系である．それは二つの論理値を表す 2 種類の異なる状態 ——否定か肯定，偽か真，あるいは単純に 0 か 1 ——のどちらかにより準備することができる．たとえば，ディジタルコンピュータで，コンデンサの平板間の電圧は情報の 1 ビットを表すことができる．すなわち，コンデンサの充電状態は 1，放電状態は 0 を表す．情報の 1 ビットは，たとえば，光の 2 種類の異なる偏光または原子の 2 種類の異なる電荷の状態を利用しても符号化することができる．いま，もしビットが 2 種類の異なる状態のどちらかに存在することができるならば，それらの**コヒーレントな重ね合わせ** (coherent superpositions) としても存在することができる，ということを

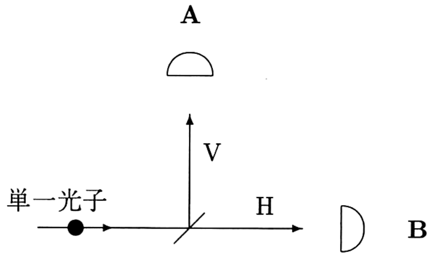


図 4.1 半透過鏡は衝突する光の半分を反射させる．しかし，単一の光子は分割しない．すなわち，そのような鏡に光子を送るとき，等しい確率で，検出器 A か検出器 B で検出される．しかし，これは光子が水平 (H) か垂直 (V) 方向のどちらかにランダムに鏡を通過することを意味しない．事実，光子は両方の経路を同時に通過する！ これは図 4.2 に示されている少し複雑な実験の助けを借りて明らかにすることができる

量子力学は述べている．これらは，一般に古典に類するものは存在せず，原子が 0 と 1 の**両方**の値を同時に表せるより進んだ状態である．物理量が二つの値を同時にもつことができるという考え方に慣れるために，図 4.1 の実験を考えることは有用である．

半透過鏡は衝突する光の半分を反射させ，残りの半分を何の影響も及ぼすことなく透過させる鏡である．図 4.1 のように，そのような鏡に一つの光子を発射してみよう．何が起こるであろうか？ わかっていることは，光子は二つに分割しないということである．すなわち，検出装置が必要な場所に光検出器を置き，光子を発射し，光検出器のどれか一つに検出され他のどの検出器にも検出されないことを確かめることができる．特に，光検出器を二つの可能な出口ビームのそれぞれの鏡の後に置くならば，光子は等しい確率でどちらかの検出器に検出される．では，光子は最初の鏡を二つの可能な方向の一つの方向に，ランダムに通過していくのであろうか？ それは間違いである！

光子は少なくともこの実験の任意の 1 回の工程で透過ビーム H か反射ビーム V の**どちらか**であることは明らかなように思えるかもしれない．しかしそれはそのどちらかではない．実際には，図 4.2 に示されている装置の助けを借りて明らかにすることができるように，光子は同時に両方の経路を通過する．両方の経路が二つめの半透過鏡で交差するように二つの普通の鏡が置か

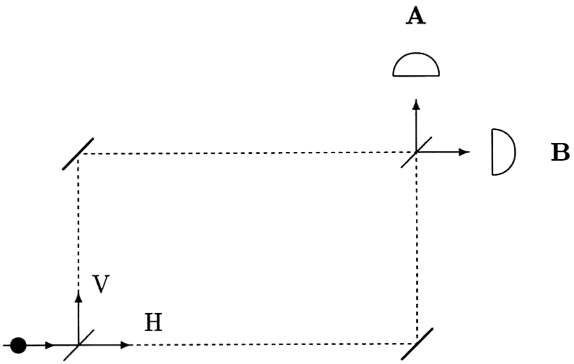


図 **4.2**　1 粒子干渉．干渉計に入る光子は常に検出器 A で検出され，検出器 B では決して検出されない．光子が干渉計を通り，一つの経路 —— H か V —— を正確に通過すると仮定するどのような説明も，実験が行われるとき検出器 A と B は平均して半分の割合でそれぞれ検出するという結論に導く．しかし実験は別のことを示している

れている．この設定により驚くべきこと——純粋に**1 粒子干渉** (single-particle interference) の量子現象——を観測することができる．

図 4.2 で，特定の光子が最初の半透過鏡に衝突後，H と書かれた水平経路に従って進んだと仮定しよう．そのとき（図 4.1 との比較により）二つの検出器は等しい確率で光子を検出することがわかる．光子が垂直経路 V 上であってもまさに同じことが観測されるであろう．よって，もし光子がそれらの装置を通り，一つの経路を正確に通過することが本当であるならば——どちらであるかは問題ではないが——実験が行われるとき検出器 A と B は平均して半分の割合でそれぞれ光子を検出するであろう．しかし，起こることはそうではない．示されている配置では，光子は常に検出器 A で検出され検出器 B では決して検出されないことがわかる．

避けがたい結論として，ある意味，光子は同時に両方の道を通過しなければならなかったということである——というのは，もし二つの経路のどちらかが吸収スクリーンにより遮断されているならば，ただちに A または B で検出される確率が等しくなる．言い換えると，経路のどちらかを遮断すること

はBを照らし出すことである．つまり，両方の経路を開くことで，光子はBに到達することを妨げる情報，鏡にぶつかりながら，まさに光子が望むように光の速さで他の経路に沿って進む情報を何とかして受け取っている．この量子干渉の性質は ——検出する粒子の運動に影響を与える目に見えないものであるように思えるが ——光子だけでなくすべての粒子やすべての物理系でも当てはまる．このように量子論は私たちのまわりで観測する宇宙よりはるかに大きな現実を述べている．この現実は，干渉現象を通してのみ互いに共存し影響し合いながら，その宇宙のさまざまな異型の近似構造を所有していることがわかる ——しかし，本稿の目的のために，この「平行宇宙 (parallel universes)」存在論について必要なことは，1粒子として見ているものは実際には非常に複雑な実体の単に一つの小さな側面であり，その残りを直接検出することはできない，という事実だけである．量子計算は粒子の目に見えない側面 ——他の宇宙に対応するもの ——を私たちに操作させることがすべてである．

もし経路HかVのどちらかで光子を遅延させるならば，量子計算で特に役立つ一つの効果を示すことができる．これは，図4.3に描かれているように，その経路上に銀のガラスを挿入することにより実現できる．光子とその目に見えない対との間の干渉はそれらの正確な到着時刻に依存するので，たとえば，光子が検出器Aの代わりに検出器Bに確実に（すなわち全宇宙に）出現するように，ガラスの厚さつまり遅延時間を選択することができる．このように，経路の一つにだけ（つまり一つの宇宙にだけ）に起こることがその両方に影響を与えている．この点についてはあとで触れることにしよう．

まさに光子は経路H上と経路V上のコヒーレントな重ね合わせとして存在することができるので，任意の量子的なビット，すなわち**量子ビット** (qubit) は，その二つの論理状態0と1の重ね合わせとして準備することができる．それは量子ビットが，任意の割合で，0と1の両方を同時に蓄えることができるということを意味している．しかし，光子が測定されるならば，ちょうど二つの経路の一つにだけ検出されるように，同様に量子ビットが測定されるならば，保持する二つの値の一つだけが，ランダムに検出されることに注意しよう．それ自身あまり役に立たない性質ではあるが．

しかしいま，数の重ね合わせのアイデアをもう少し進めてみよう．3物理ビットから構成されるレジスタを考えてみよう．古典的な3ビットレジスタ

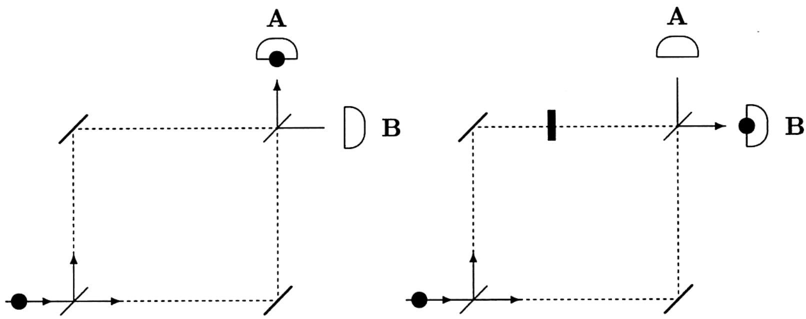


図 4.3　干渉計の二つの経路の一つに挿入された銀のガラスは一つの検出器から別の検出器へ光子の方向を変えることができる．左の干渉計に入るすべての光子は検出器 A で検出される．右の干渉計では，干渉は垂直経路上の銀のガラスにより修正され，結果としてすべての光子は検出器 B に到達する．このように一つの経路にだけに起こったことが，確実に実験の最終結果を変えている．この効果は特に量子計算で役に立つ

は正確に 8 個の異なる数の一つを蓄えることができる．すなわち，レジスタは数 0 から 7 を表す 8 個の可能な構成 000, 001, 010, . . . , 111 の一つとして存在することができる．しかし，3 量子ビットから構成される量子レジスタは量子重ね合わせにより 8 個の数まで同時に蓄えることができる．8 個の異なる数が同じレジスタに物理的に存在できるということはまったく注目すべきことである．しかし，数 0 と 1 の両方が同じ量子ビットに存在できることに比べれば驚きは小さいであろう．もしさらに量子ビットをレジスタに追加するならば，量子情報を蓄えるその容量は指数的に増加する．すなわち，4 量子ビットは同時に 16 個の異なる数を蓄えることができ，一般に L 量子ビットは同時に 2^L 個までの数を蓄えることができる．250 量子ビットのレジスタは ——本質的に 250 個の原子から構成されているといえるが ——知られている宇宙の原子より多くの数を同時に保持することができるであろう（むしろ，これはそれらが保持する量子情報の量を控えめに言っている．というのは，一般に重ね合わせの要素は連続的に変化し，さらにそれぞれ自身の位相角をももっているからである）．たとえそうであっても，もしレジスタの内

容を測定するならば，これらの数の一つだけしか見られないであろう．しかし，いまある自明でない量子計算を実行することができ，ひとたびレジスタを多くの異なる数の重ね合わせとして準備するならば，それらのすべてに同時に数学的な演算を実行することができる．

たとえば，もし量子ビットが原子ならば，そのとき適宜回転するレーザパルスがそれらの電子状態に作用し，符号化された数の初期重ね合わせを別の重ね合わせに発展させる．そのような発展の間，重ね合わせのそれぞれの数に作用し，大規模な並列計算を実行していく．このように，量子コンピュータは1計算ステップで，2^L 個の異なる入力数に，同じ数学的な演算を実行することができ，結果としてすべての対応する出力の重ね合わせになる．同じことを実現させるためにどんな古典コンピュータでも 2^L 回の計算を繰り返すか，並列に実行する 2^L 個のプロセッサを使わなければならない．このように，量子コンピュータは時間やメモリといった計算資源の使用について ── ある種の計算だけではあるが ── 莫大な利益を与える．

4.1.3 量子アルゴリズム

どのような種類の計算か？　話してきたように，従来の情報記憶装置はそのようなものではない．なぜならコンピュータは，いま 2^L 個の計算のすべての結果を保持するのではあるが，物理法則は単にそれらの一つだけしか見ることを許していないからである．しかし，ちょうど図4.2の実験の唯一の答え「A」が二つの経路のそれぞれに沿って伝わった情報に依存するように，量子干渉は唯一の結果，全 2^L 個の中間結果に論理的に依存する最終結果が得られることを可能にする．

この考えを基にしてニュージャージー州のAT&Tベル研究所のLov Groverにより最近発見された注目すべき量子アルゴリズム [120] は，N 項目のソートされていないリストをわずか $\sqrt{N}$ ほどのステップ数で探索する信じがたい離れ業を達成している．たとえば，名前がアルファベット順にコンピュータメモリに蓄えられている100万項目を含む電話帳から特定の電話番号を探すことを考えてみよう．与えられた番号が見つかるまで単に項目を一つひとつ調べていく総当たり法 (brute-force method)，これは平均で500,000メモリのアクセスを必要とするであろうが，これより良くすることができる古典アルゴリズムが存在しないことは簡単に確かめられる（また明らかである）．量子

コンピュータは，ただ1回のアクセス時間で，すべての項目を同時に調べることができる．しかし，その時点で単に結果を印刷するようにプログラムされているならば，古典アルゴリズムより良くなることはない．すなわち，単に百万の計算経路の一つ（すなわち100万宇宙の一つ）だけが探している項目と照合するだけで，そこでコンピュータの状態を測定したならば，その情報を得ることはほんの100万分の1の確率であろう．しかし，もしそのコンピュータの量子情報を，測定せずに残しておくならば，続く量子演算により，ちょうど上で述べられた単純な干渉実験のように，その情報を他の経路に作用させることができる．この方法により，要求された項目の情報が量子干渉を通して，より多くの宇宙に広められる．もしこの干渉を生成する演算が約1000回（一般に，$\sqrt{N}$回）繰り返されるならば，要求される番号を含む項目の情報が確率0.5となり測定しやすくなるであろう ——すなわち，全宇宙の半分以上に広まったであろう．それゆえ全体のアルゴリズムをあと数回余分に繰り返すことで，ほとんど1に近い確率で要求される項目を見つけられるであろう．

与えられた性質をもつ項目を見つけるのに加え，Groverの探索アルゴリズムはその応用としてリスト内の最大値や最小値，あるいはモード値なども見つけることができ，非常に用途の広い探索ツールである．しかし実際には，物理的なデータベースを探索することはGroverのアルゴリズムの主な利用方法ではない ——少なくとも古典メモリが量子メモリより安価である限りにおいては．というのは，データベースを古典メモリから量子メモリへ（ビットから量子ビットへ）変換する演算はそれ自身$O(N)$ステップを必要とするので，Groverのアルゴリズムは探索時間を最良で定数倍しか改善しないが，これは古典並列処理によっても達成することができる．Groverのアルゴリズムが本当に対象としていることは**アルゴリズム的探索** ——つまり，メモリに蓄えられているのではなく，計算プログラムの実行中に自身で生成するリストの探索 ——である．たとえば，チェスをする古典コンピュータでは，ある与えられた位置から大雑把に（やみくもに「総当たり」探索を使い）100万手調べるのに要するステップ数で量子コンピュータは1兆の可能な次の手を調べるこのアルゴリズムを使うことができる．古典的なチェスのアルゴリズムで「枝刈り (tree-pruning)」によるより大きな見通しが得られるにもかかわらず，これは非常に重要な改善を与えるであろう．

モントリオール大学の Gilles Brassard が最近指摘したように [121]，Grover のアルゴリズムの別の重要な応用は，DES（Data Encryption Standard，量子暗号については第 2 章を参照）などの古典暗号の枠組みを攻撃する，暗号解読としてであろう．DES を破ることは本質的に $2^{56} = 7 \times 10^{16}$ 個の可能な鍵の探索を必要とする．もしこれらが 1 秒当たり百万鍵の割合でチェックすることができるならば，古典コンピュータが正しい鍵を発見するまでに 1000 年以上必要なところが，Grover のアルゴリズムを使う量子コンピュータでは 4 分以内で見つけることができるであろう！

ある奇妙な一致により，量子コンピュータの優れた特徴のいくつかは暗号についての応用を備えている．それらの一つが Grover のアルゴリズムである．他の一つが Peter Shor ——彼もまたニュージャージー州の AT&T ベル研究所所属であるが ——により 1994 年に発見された大きな整数を効率的に素因数分解する量子アルゴリズムである [36]．この量子と古典アルゴリズムの性能の差はさらにめざましいものがある．数学者は 10 進で N 桁の数を素因数分解するために，どんな古典コンピュータを用いても N の指数的に増加するステップ数を必要とすると（実際に彼らは証明してはいないのではあるが，固く）信じている．すなわち，素因数分解される数を一桁増やすことは一般に要求される時間に定数因子を掛けるということである（4.2 節参照）．このように，桁数を増加させると，その作業は急速に手に負えなくなってくる．数学上の挑戦として素因数分解させられた最も大きな数，つまり，数学者に挑戦するために別の数学者によりその素因数が秘密裏に選ばれた数は 129 桁であった．古典的な手段で 1000 桁の数をどのように素因数分解するかはだれも想像することさえできない．その計算は宇宙の推定年齢と同じくらい長い時間を必要とするであろう．これに対し，量子コンピュータは秒単位で 1000 桁の数を素因数分解することができる ——そして実行時間は単に桁数の 3 乗程度の割合で増加するのみある．

今日，素因数分解の困難さは現在最も信頼されている暗号化手法，特に RSA(Rivest, Shamir, Adleman) 系 ——これはよく電子銀行口座を保護するために用いられている [122]（詳細は第 2 章参照）——の安全性を裏付けている．ひとたび量子素因数分解エンジン（大きな数を素因数分解する特殊目的用量子コンピュータ）が作られるならば，そのような暗号系のすべてが安全でなくなるであろう．

計算を実行するための量子現象の潜在的な能力は，1981 年に MIT で開催された第 1 回計算物理の会議 (First Conference on the Physics of Computation) で，Richard Feynman の話の中で最初に輪郭が示された．彼は量子系の発展を古典コンピュータにより効率的な方法で模倣することは一般に不可能であるように思えることを考察した [123]．発展する量子状態を記述するために要求される古典情報量は，同等の精度で対応する古典系を記述するために要求されるものより指数的に大きいので，本質的に量子発展のコンピュータによる模倣は，実際の発展と比較して，概して指数時間の遅延がある（干渉効果を予測するために，平行宇宙のすべての系において指数的に多くの対応するものを記述しなければならない）．しかし，この手に負えなさを障害と見るかわりに，Feynman はそれを好機と見なした．彼は，もし多粒子干渉実験で発生することを実行するほどの大きな計算を要求するならば，そのような実験装置を組み立て，結果を測定するまさにその行為は複雑な計算を実行することに等しい，ということを指摘した．

量子計算は，単純な場合に —— 量子系の振る舞いを予測するために —— すでに利用されてきている．近い将来のある時点において，それは科学の構造に新しくかつ置き換えることができない役割を獲得するであろう．なぜなら予測するという科学の能力がそのとき量子計算に依存するであろうからである．

計算の量子論の基礎は（それは現在，計算の理論**そのもの** —— Turing の古典理論は単に近似である —— と見なされなければならないが），オックスフォード大学の David Deutsch が**万能量子コンピュータ** (universal quantum computer) を記述した非常に重要な理論の論文を出版した 1985 年に構築された [124]．そのとき以来，量子コンピュータについてなすべき興味深い事柄や，また同時に，量子コンピュータを構築するための科学的かつ技術的発展が探し求められている．

4.1.4　量子コンピュータの構築

原理的には，私たちは量子コンピュータの作り方を知っている．つまり，単純な量子論理ゲート（第 1 章参照）から始め，それらを量子ネットワークとして接続すればよい．

量子論理ゲートは古典ゲートと同様に，一般に 2 量子ビット上で，所定の時

間内に一つの基本的な量子演算を実行する非常に単純な計算素子である [125]．もちろん，量子論理ゲートは量子重ね合わせ上で演算を生成し実行することができるので古典的なものと異なっている．しかしネットワーク内の量子ゲートの数が増加していくとき，ただちにある重大な現実的問題に直面する．相互作用する量子ビットが多くなればなるほど，量子干渉を起こす相互作用を設計することがますます困難になる傾向がある．1 原子や 1 光子の尺度で操作する技術的難しさを除けば，最も重大な問題の一つはまわりの環境が量子重ね合わせを生成する相互作用により影響されるのを防ぐことである．構成要素が多くなればなるほど，このように計算を阻害しながら，ますます量子情報は量子コンピュータの外に拡散し，環境の中に失われていくように思われる．この過程は**デコヒーレンス** (decoherence) と呼ばれ，詳細は第 7 章で議論される．このように，私たちの仕事は量子ビットが互いに影響を及ぼし合うが，環境とは影響を及ぼし合わないサブミクロ系を設計することである．

ある物理学者たちは，量子コンピュータ技術における実質的なさらなる進歩の見通しについて悲観的である．彼らは，数ステップの連続する量子計算を実行できる程度しかデコヒーレンスは実際には減らせないであろうと信じている（ついでながら，これについてはすでにいくつかの非常に役に立つ素子が見込まれている. 表 4.1 参照）．他方，より楽観的な研究者たちは，実際の量子コンピュータはおよそ数十年ほどで出現するであろうと信じている．私たちは楽観的に考えがちである．なぜなら一部は，理論は現在途中に根本的な障害となるものはなく，量子エラー訂正やフォールトトレラント計算（第 7 章参照）が可能であるといい，一部は現在このプロジェクトで働いている実験物理学者たちの驚くばかりの才能や問題解決能力に感謝し，また一部は楽観主義は事を起こさせるからである．

しかし，問題は一挙に解決されないであろう．現在の挑戦は十分完成した万能量子コンピュータをいますぐ作ることではなく，むしろ量子現象を単に観測するという実験からこれらの現象を必要な方法で制御可能にする実験へ移行することである．2 量子ビットを含む単純な量子論理ゲートはヨーロッパやアメリカ合衆国で実験室において実現されてきている．次の 10 年は数量子ビット以上を制御することであり，疑いもなく，すでに自然を利用する新しい方法を活用し始めている．たとえば，単純な量子ネットワークはより良い周波数標準を与えることが知られている [126]（7.6 節参照）．量子コン

表 4.1　量子コンピュータ技術の発展の指標

ハードウェアのタイプ	必要とする量子ビット数	デコヒーレンスまでのステップ数	現状
量子暗号	1	1	実装
エンタングルメントを用いた量子暗号	2	1	デモ
量子 C-NOT ゲート	2	1	デモ
複合ゲート	2	2	デモ
Deutsch のアルゴリズム	2	3	デモ
通信路容量 2 重化	2	2	まもなく実現
テレポーテーション	3	2	デモ
エンタングルメント・スワッピング	4	1	デモ
量子暗号のための中継局	数個	数個	理論が不十分
量子シミュレーション	数個	数個	簡単なデモ
単純なデータを用いた Grover のアルゴリズム	3+	6+	NMR を用いたデモ
高精度周波数標準	数個	数個	近い未来
エンタングルメント精製	数個	数個	近い未来
単純なデータを用いた Shor のアルゴリズム ...	16+ ...	数百+ ...	
量子素因数分解エンジン	数百	数百	
万能量子コンピュータ	数千+	数千+	

ピュータ技術の発達におけるいくつかの起こりうる重要な項目が表 4.1 に示されている．

4.1.5　より深い洞察

1970 年代に計算物理について最初に体系的に調査されたとき，主な不安材料は物理対象がビット，論理ゲート，演算要素などの特性を実現する精度に対し量子力学的効果が基本的な制限を与えるかもしれないということで，このことは抽象的かつ数学的に洗練された計算の理論の中に表れている．すなわち，その理論の能力と上品さ，計算の普遍性といった深遠な概念，Turing の停止定理といった深遠な結果，さらにすぐれた現代計算量理論はすべて単に純粋数学の虚構であり，実際に自然と何の関係もないかもしれないということが懸念された．

これらの不安材料はいままで述べてきた研究により意味もなく容認されていただけでなく，それぞれの場合，ほんの20年前のことだということをだれも夢にも思わないほどその基礎をなす考えが不思議にも擁護されてきた．説明してきたように，量子力学は古典計算がいったい何を実行できるのかという制約から離れ，それらすべてを許容し，加えて古典コンピュータがまったく実行することができない（完全に安全な公開鍵暗号などの）タスクを実行するアルゴリズムを含め，まさに計算の新しい様式を与える．理論の上品さに関する限り，その分野の研究者は現在，古典的な近似ではいままで期待することができなかったほど，現実の計算理論は他の分野の基本的な理論とよりうまく融合し，はるかに自然に調和している，という事実に慣れるようになってきている．最も単純なレベルにおいてさえ，まさに「量子」という言葉は「ビット」という言葉と同じこと —— 基本的な量 —— を意味し，そしてこのことが完全に古典物理系は「カオス」として知られている包括的な不安定性に従っており，ディジタル計算をまったく裏付けるものではないという事実を反映している（Turing 機械，すべての古典コンピュータの理論的プロトタイプでさえ，ひそかに初めから量子力学的であった！）．古典理論のChurch-Turing の仮説（すべての「自然な」計算のモデルは本質的に互いに等価である）は決して証明されなかった．計算の量子論についてその対応するもの（Turing の原理，万能量子コンピュータは任意の有限物理系のふるまいを模倣することができるということ）は直ちに Deutsch の 1985 年の論文で証明された [124]．より強い結果（これもまた古典的な場合に予想されてはいるが決して証明されていないもの），すなわち，そのような模倣が常に物理的な発展に要する時間の高々多項式関数の時間で実行できるということが，その後量子的な場合に証明された．

明らかに距離の離れた研究分野における量子計算の多くの支流の間において，哲学と数学的証明の実現の両方と密接な関係がある．決められた出力をもつ計算を実行することは，その観測された出力が与えられた計算の可能な結果の一つであるということを**証明する**ことと等価である．コンピュータの演算を数学的に記述することができるので，そのような証明を常にある数学上の定理の証明に翻訳することができる．このことは古典的な場合でも同様であるが，干渉効果がない場合，常に計算のステップを書き留めねばならず，その結果，古典的な定義を満足させる証明 —— 標準的な推論規則により順番

に公理か以前の命題の補足といった一連の命題 —— を生成する．いまその定義を破棄しなければならない．これからは，証明は過程と見なされなければならない —— 計算それ自身は全ステップの記録ではないのではあるが —— というのは，もしそのような証明に対応する「命題の列」が印刷されるならば，その紙はその観測可能な宇宙を何度もいっぱいにするので，将来，人間の脳や他のどんな全権を委任された機関でも 1 ステップごとチェックすることができない手段で量子コンピュータが定理を証明するであろうことを受け入れなければならない．量子計算のより深い洞察についてのより包括的な議論については文献 [127] で見つけだせる．

4.1.6　おわりに

量子計算の実験的および理論的研究は，現在世界中の研究者や産業界からますます注目されてきている．量子レベルで自然が制御されかつ操作することができるというアイデアは物理学者や技術者の想像力に強い刺激を与えている．古典的なものを超えて数々の利点を備えた量子計算や新しい量子アルゴリズムを実現するためのより有望な技術の開発は日々進歩している．ここに真に革命的な技術革新が内在している．

本稿は *Physics World* の 1998 年 3 月号に掲載された量子計算の紹介論文 [128] の改定版である．

4.2　量子アルゴリズム

(*R. Jozsa*)

4.2.1　はじめに

量子アルゴリズムは，有用な計算タスクを実行するために，特徴として量子効果を利用する任意の物理過程である．これらの量子計算処理の記述を古典計算の形式化と密接に対応させるモデルとして形式化すると都合がよい．本質的に，コンピュータのメモリビットはビットよりむしろ量子ビットであり，基本演算は古典計算におけるブール演算よりむしろ有限定数個の量子ビット上でそれぞれ演算するユニタリ変換である．この種のモデルが任意の一般的な量子物理過程を記述するために十分であるかということが議論されるかもしれない [124]．任意の計算は「有限手段」により演算することを要求され

る．すなわち，それは基本ユニタリ演算のある決められた有限集合内の任意の演算を適用できるということだけを備えている．アルゴリズムで必要な他の任意の演算は選択された量子ビット上でこれらの基本単位から動作を組み合わせることにより構成されなければならない（あるいはむしろ十分な精度で近似されなければならない）．いくつかのとても小さなユニタリ演算の集まり（いわゆる演算の「万能集合」）が，任意の量子ビット数上で任意のユニタリ演算を任意の精度で近似するために十分であることが示されている [129, 130].

この形式化の最も有用かつ重要な結果の一つは，計算タスクの複雑さを（これもまた古典計算量理論の概念との対応により）評価する方法を与えていることである．特に時間計算量，すなわち計算タスクを完了するために必要な基本演算の数を入力サイズの関数として評価することに関心をもつであろう．

二つのコンピュータ A と B が異なる（万能）基本演算集合を備えているならば，任意の計算タスクの時間計算量は一般に異なるであろう．しかし，B はまず A の各基本演算を B 自身の演算集合を用いてプログラムし，そして A の演算集合で書かれた任意のプログラムを実行してもよい．B が A の基本演算の任意の一つをまねるのに要する最大のステップ数を k とする．そのとき任意の計算タスクに対する B 上の時間計算量は A の時間計算量の高々k 倍である．すなわち，基本演算集合の変更は任意の計算タスクに対し（入力サイズに無関係に）高々定数倍遅くなるにすぎない．計算量理論では，一般に計算の正確なステップ数に興味があるのではなく，むしろ入力サイズの増加に伴う特有のステップ数の増加の割合に興味がある．実際，一般にステップ数が入力サイズの多項式関数で制限されている（いわゆる多項式時間アルゴリズムまたは効率的なアルゴリズムが与えられている）か否か，あるいは入力サイズに伴い指数的（超多項式的）に増加するか否かということだけを問題にしている．上記の注意点に従うと，この相違はコンピュータの選択とは無関係であり，計算タスク自身の固有の性質である．

量子アルゴリズムの研究において，古典多項式時間アルゴリズムが知られていない問題に対し多項式時間アルゴリズムを見つけることは最大の関心事である．すなわち，量子効果が古典情報処理に対し実行時間において指数倍の高速化を可能にするかもしれないということを示したい．このことを示唆するさまざまな状況 —— Deutsch, Simon, Shor のアルゴリズム —— につい

て述べる．また任意の古典アルゴリズムに対し指数倍の高速化というよりむしろ平方根の高速化を与える Grover の量子探索アルゴリズムについても述べる．これはかなり実用的な関心事であるが，Grover のアルゴリズムはまた NP と呼ばれる古典計算量クラスと関係しており，理論的な対象にもなっている [131, 132].

任意の拡張された量子アルゴリズムを将来実装することは，現在，非常に実験的な挑戦であることが第 5 章でわかるであろう．しかし興味深い量子アルゴリズムが存在するということは，単に理論的構成のレベルにおいても，古典物理と量子物理の基本構造の間で新しい本質的な相違を表しているのでそれ自身大きな価値がある．情報処理の観点からは，計算量理論の概念的枠組みを用い定量化することができるということで，量子物理学の時間発展は古典的な時間発展より本質的により複雑であると思われる．

上に挙げた量子アルゴリズムにおける計算の高速化で現れる本質的な量子力学的効果は，量子**エンタングルメント** (entanglement) のさまざまな性質に由来する．そのような支配的な役割を演じる二つの効果について議論を始めよう．それらは「量子並列計算 (quantum parallel computation)」（4.2.2 項）と「局所演算の原理 (principle of local operations)」（4.2.3 項）と呼ばれている．

4.2.2　量子並列計算

関数 $f : A \to B$ を考えよう．ただし A, B は有限集合である．典型的な例として，A と B は Deutsch や Simon のアルゴリズムのように（ある n に対し）すべての 2^n 個の n ビット列の集まりであってもよいし，Shor のアルゴリズムのように $\mathcal{Z}_N$,（ある N に対し）N を法とする整数の集合であってもよい．ここでは，A と B をアーベル群とする．$\mathcal{H}_A$（または $\mathcal{H}_B$）を A（または B）の要素によりラベル付けされた直交基底をもつヒルベルト空間とする．量子計算では，f の計算は慣例により $|a\rangle|b\rangle$ を $|a\rangle|b \oplus f(a)\rangle$ に変換する $\mathcal{H}_A \otimes \mathcal{H}_B$ 上の演算であるユニタリ変換 U_f に対応する（図 4.4 参照）．ここで $\oplus$ は B におけるアーベル群上の演算を表す．

$\mathcal{H}_A$ は入力レジスタの状態空間であり，$\mathcal{H}_B$ は出力レジスタの状態空間である．入力 $|a\rangle$ は U_f がすべての可能な f に対しユニタリであることを保証するように実行される．もし b がはじめ 0 に設定されているならば，$f(a)$ は与えられた基底における標準的測定により出力レジスタから直接読み取れる．

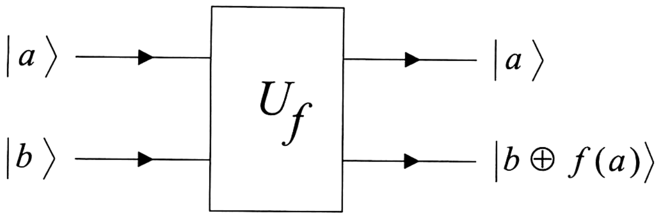


図 4.4　関数 f の評価に対応するユニタリ変換 U_f の量子ゲート図．上下の線はそれぞれ入力と出力レジスタを表す

いま入力レジスタが値の重ね合わせ，均等な重ね合わせ $\sum_{a \in A} |a\rangle$ （ここで正規化因子は省略）により設定されていると仮定しよう．そのとき $b = 0$ で U_f を適用すると，量子発展の線形性により，出力の重ね合わせ $\sum |a\rangle|f(a)\rangle$ を得る（図 4.5 参照）．

U_f をちょうど **1** 回実行するだけで，重ね合わせにより f のすべての値が計算できる．これは，[124] で Deutsch により導入された，量子並列計算 (quantum parallel computation) の処理である．出力状態 $\sum |a\rangle|f(a)\rangle$ は一般に入力と出力レジスタのエンタングルした状態である．実際，重ね合わせの現象はまた古典線形系の特徴でもあり，重ね合わせだけに依存する任意の効果は古典系において容易に実現することができる．しかし，量子エンタングルメントの現象には古典的に対応するものはなく，量子計算におけるその基本的な役割が [133, 134] で強調され詳しく調べられている．

$B = \{0, 1\}$ を 2 を法とする整数の加群とし，$\mathcal{B}$ により 1 量子ビットのヒルベルト空間，すなわち $\{|0\rangle, |1\rangle\}$ により表される標準基底を備えた 2 次元ヒルベルト空間を表すものとする．$\mathcal{B}^n$ はすべての n ビット列によりラベル付けされた基底 $\{|x\rangle : x \in B^n\}$ を用いて n 量子ビットの 2^n 次元ヒルベルト空間

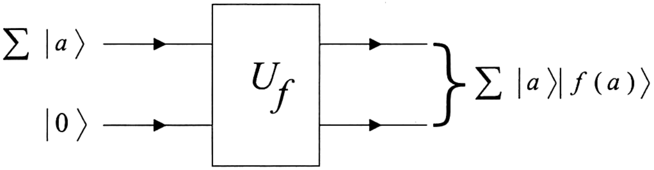


図 4.5　量子並列計算

$\mathcal{B}\otimes\cdots\otimes\mathcal{B}$ を表す．H を基本的な1量子ビットのユニタリ演算

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{4.1}$$

とする．このとき，

$$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{4.2}$$

となる．

関数 $f:B^n\to B$ を考えよう．量子並列による計算の例として，以下のようにすべての入力値の重ね合わせを設定し，f のすべての値を重ね合わせにより計算しよう．

(i)　n（入力）量子ビットの標準状態 $|0\rangle\ldots|0\rangle$ から開始し，H を各量子ビットに別々に適用させよ．これは以下の状態になる．

$$\frac{1}{2^{n/2}}(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle)=\frac{1}{2^{n/2}}\sum_{x\in B^n}|x\rangle \tag{4.3}$$

(ii)　さらに1（出力）量子ビットを状態 $|0\rangle$ として追加し，以下の状態を与える U_f を適用させよ．

$$|f\rangle=\frac{1}{2^{n/2}}\sum_{x\in B^n}|x\rangle|f(x)\rangle \tag{4.4}$$

(i) はほんの $O(n)$ 個の演算だけを必要とし，それは n の多項式であるが，式 (4.4) で f の**指数的に**多くの値の重ね合わせを導くことに注意しよう．

量子エンタングルメントはまた，重ね合わせの表現において別の重要な役割も演じている．もし古典的に 2^n 個のモードの一般的な重ね合わせを作りたいならば，各モード，たとえば振動系の振動の 2^n 個のモードを維持することができる**一つの**系を必要とする．これらのモードはある物理資源の非常に高い準位，たとえば振動系のエネルギーに対応し，そのとき 2^n 個のモードの一般的な重ね合わせはそれを表現するために物理資源の（n の）指数倍の量を必要とする．これに対し，量子論では n 個の2準位系を用い，2^n 個の状態の重ね合わせを —— **エンタングルメントの現象のために** —— 表すことができる．一般的なそのような重ね合わせはいま，高々n 個の系のそれぞれが別々

に励起する必要があるだけなので，それを表すために物理資源の**線形倍**の量だけを必要とする．すなわち，重ね合わせは古典系でも生成できるが，量子エンタングルメントの現象は大きな重ね合わせを表すために必要とされる物理資源を指数的に節約している．

4.2.3 局所演算の原理

古典あるいは量子のいずれにおいても，すべての計算で処理される情報はコンピュータ（の部分）の物理状態自身に表れる．n 古典ビットの状態自身の記述をその量子的に対応するもの，n 量子ビットの状態と比較してみよう．n ビットは指数的に多くの状態の任意の一つとして存在することができるのではあるが，各状態はちょうど n ビットの情報を与えることにより完全に記述することができる．これに対し，一般の n 量子ビットの（エンタングルした）状態は，列挙が必要な指数的に多くの重ね合わせ成分を含んでもよい．この意味において, 量子系はその古典的なものより指数的により多くの情報を表すことができる．これは量子振幅が連続領域の値をとることができるという事実の結果ではない —— たとえ振幅を数のある単純な基本集合に制限したとしても成り立つ．たとえば, 式 (4.4) の $(n+1)$ 量子ビット状態 $|f\rangle$ は，関数 f への指数個もあるすべての入力値に対する出力 0/1 の値の情報を表す．n 量子ビットのエンタングルしていない（積の）状態を記述するために必要な情報は単に n の線形倍，1 量子ビット状態を記述するために必要な情報の n 倍，増加するだけであることに注意しよう．

量子力学の形式化では，どんな古典的な手段でも実時間で比較することができないほど，量子状態の膨大な情報量を効率的に処理できる．量子論のこの著しい特徴は [123] で Feynman により最初に指摘された．あるエンタングルした状態 $|\psi\rangle$ を n 量子ビットの物理系とし，第 1 量子ビットに 1 量子ビットの演算 U を適用すると仮定しよう．これは量子計算で 1 ステップとして（あるいはむしろ，もし U がコンピュータにより与えられる他の基本演算から組み立てられる必要があるならば，n に独立な定数ステップ数として）計数されるであろう．いまその状態でこの情報処理に対応する古典計算を考えてみよう．$|\psi\rangle$ は各下付き添え字が 0 または 1 の（n 量子ビットの積の基底に関係する）成分 $a_{i_1\cdots i_n}$ として記述してもよく，U は 2×2 のユニタリ行列 U_i^j に

より表せる．U の適用は行列の積

$$a_{i_1\cdots i_n}^{(\text{new})} = \sum_j U_{i_1}^{j} a_{j i_2 \cdots i_n} \tag{4.5}$$

に対応する．このように 2×2 行列の積は，列 $i_2 \cdots i_n$ の各可能な値に対し一度ずつ 2^{n-1} 回実行される必要があり，n の**指数的**に増加する計算量を必要とする．量子コンピュータでは，エンタングルメントのため，この 2^{n-1} 回の繰返しが不要である．これが「局所演算の原理 (principle of local operations)」である．すなわち，大きなエンタングルした系の部分系上でたった一つの局所ユニタリ演算が，一般に古典計算状態を表すために指数的な作業を必要とする量の情報を処理する．

上で指摘した意味において，n 量子ビットは情報を表すために n 古典ビットより指数的に大きな容量をもっている．しかし，量子状態として表される潜在的に膨大な情報はさらに注目すべき特徴を備えている —— そのほとんどはどんな可能な手段を用いても**取り出すことができない**！　実際，量子観測理論は与えられた未知の量子状態自身について得ることができる情報量にきびしい制約を置いている．情報のこの内在する取得不可能性は Shannon の情報理論の言葉 [137] で定量化されてもよい [135, 136]．一般の n 量子ビットの状態の場合，その $O(2^n)$ 個の情報内容から，たとえどんな物理手段を用いても，その状態の一つのコピーからは高々n 古典ビットの情報だけしか抽出されない．これは n 古典ビットの最大情報容量と一致する．

与えられた未知の量子状態の完全な（主に取得できない）情報内容は量子情報と呼ばれる．一般的な量子物理的発展は量子情報処理と考えられる．したがって，計算量の観点からは古典と量子物理の間の新しい一風変わった相違を表す．すなわち，一般的な量子物理的発展を実行するために，自然はどんな古典的な手段を用いても実時間で比較できないほど膨大な情報量を処理しなければならないが，同時に，この処理される情報のほとんどは私たちから隠され続けている！　しかしこの量子情報の内在する取得不可能性は，役に立つ計算のための高性能な情報処理能力を探求していくことを排除するものではないことを指摘しておくことは重要である．実際，古典的な手段ではなお指数的な作業を必要とする最終状態の包括的な性質が少ない情報量で抽出されるかもしれない．上で述べた量子並列計算の技術は一つの例である．す

なわち，式 (4.4) の状態 $|f\rangle$ の完全な量子情報はすべての個々の関数値 $f(x)$ の情報を含んでいるが，どんな測定を用いてもすべてを取り出すことはできない．しかし，すべての関数値の集まりからある包括的な性質が $|f\rangle$ 上で標準基底 $\{|x\rangle, |y\rangle\}$ に直交していない測定により決定される**かもしれない**．たとえば，もし f が周期関数ならば，個々の関数値を特徴付けることはまったくできないが，古典的な手段では，確実に結果を得るためには一般に指数的な数の関数評価を必要とする周期の値を包括的な性質により決定できるかも知れない．これは Shor の効率的な量子素因数分解アルゴリズムの仕組みの鍵となる（4.2.6 項参照）．

一般的な言葉により量子論がいくつかの基本的な計算に役立つことを議論してきたが，これから種々の基本的な量子アルゴリズムの仕組みについて述べていこう．

4.2.4 オラクルと Deutsch のアルゴリズム

Deutsch のアルゴリズム [124, 138] は，量子効果を用いることによりどんな古典的手段より指数倍高速に実行することができる計算タスクの最初の例であった．その後 [139] で改良され，ここでは最も最新の形を記述する．

まず四つの可能な 1 ビット関数 $f : B \to B$ を考えよう．二つの定数関数

$$\begin{matrix} f(0)=0 \\ f(1)=0 \end{matrix} \quad \text{または} \quad \begin{matrix} f(0)=1 \\ f(1)=1 \end{matrix} \tag{4.6}$$

と，二つの「等分」関数（出力値 0 と 1 が等しく生じるという意味で等分されている）

$$\begin{matrix} f(0)=0 \\ f(1)=1 \end{matrix} \quad \text{または} \quad \begin{matrix} f(0)=1 \\ f(1)=0 \end{matrix} \tag{4.7}$$

がある．いま，これらの関数の（未知の）一つを計算する「ブラックボックス (black box)」または「オラクル（oracle，神託）」が与えられていると仮定しよう．オラクルは任意に与えられた入力値（または図 4.5 のような入力の重ね合わせ）に対し，関数の値を与える封印された箱（図 4.4 参照）として描かれるかもしれない．またはオラクルを，文や内部の仕組みを検査することが許されていない実行可能なコンピュータサブルーチンと見なしてもよい（後に f の評価に対するこの呼び出しの制約についての重要性を議論する）．問題は，オラクルにより計算される関数が等分か定数かを決定することである．

古典計算の状況では，確実に問題を解くために明らかにオラクルに 2 回質問する必要がある．実際，関数の一つの値だけ（すなわち $f(0)$ か $f(1)$）しか知らないならば，関数が等分か定数かについての情報をまったくもっていない！　次に，量子コンピュータでこの問題がちょうど 1 回のオラクルへの質問だけで確実に解かれることを示す．

（上述したように）量子並列計算の能力を付加的な工夫 —— 出力レジスタをまず $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ に設定する —— を行って利用する．量子計算は以下のように実行する．入力と出力レジスタの標準状態 $|0\rangle|0\rangle$ から始め，出力に NOT 演算，そして両方のレジスタに H を適用し

$$\begin{aligned} |0\rangle|0\rangle \to |0\rangle|1\rangle \to \quad & \left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ & = \tfrac{1}{\sqrt{2}} \textstyle\sum_{x\in B} |x\rangle \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \end{aligned} \tag{4.8}$$

を得る．次にこの状態をオラクルに与える．すなわち U_f を適用する．U_f は $|x\rangle|y\rangle$ を $|x\rangle|y \oplus f(x)\rangle$ に変換することを思い出すと

$$\mathcal{U}_f : |x\rangle(|0\rangle - |1\rangle) \to \begin{cases} \ \ |x\rangle(|0\rangle - |1\rangle) & f(x) = 0 \text{ のとき} \\ -|x\rangle(|0\rangle - |1\rangle) & f(x) = 1 \text{ のとき} \end{cases}$$

であることがわかる．よって

$$\mathcal{U}_f : \frac{1}{\sqrt{2}} \sum_{x\in B} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \to \left(\frac{1}{\sqrt{2}} \sum_{x\in B} (-1)^{f(x)} |x\rangle\right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{4.9}$$

となる．この処理を通じて出力レジスタは状態 $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ のままである．入力レジスタは状態 $\frac{1}{\sqrt{2}}\sum_{x\in B}(-1)^{f(x)}|x\rangle$ となる．もし f が定数関数ならば $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ を得，もし f が等分関数ならば $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ を得る．いま H は自分自身の逆演算である．すなわち，$HH = I$ であることを直接確かめることは簡単である．こうして最後に H を入力レジスタに適用し（(4.2) に注意すると），もし f が定数ならばこのレジスタの状態は $\pm|0\rangle$ になり，f が等分ならば $\pm|1\rangle$ になる．これらは標準基底での測定により確実に区別でき，ちょうど 1 回のオラクルへの質問の後，確実に等分と定数関数を区別する．全体の演算の列は，図 4.6 に示すネットワークダイアグラムにまとめられている．

上記のオラクルへの 1 回と 2 回の呼び出しの違いは形式的な計算量の考察に対し直接重要性をもたないが，上の処理のアイデアを古典と量子の解の間の**指数的分離**をまさに示す状況へすぐに一般化できる．

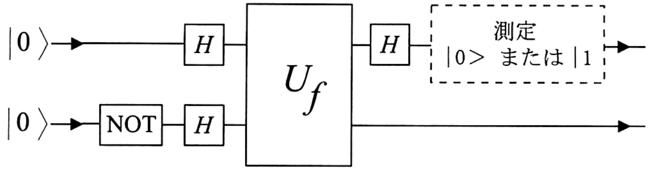


図 4.6 1 ビット関数の Deutsch のアルゴリズム．0（または 1）の測定値は f が定数（または等分）であることを知らせる

1 ビットから 1 ビットへの関数の代わりに n ビットから 1 ビットへの関数

$$f : B^n \to B$$

を計算するオラクルが与えられていると仮定しよう（そして n の値も知っているとする）．関数は定数（すなわち 2^n 個の値がすべて 0 かすべて 1）か等分かであると約束されている．ここで等分とは，正確に半分（すなわち 2^{n-1} 個）の値が 0 であり半分が 1 であることを意味する．$n > 1$ に対し n ビットから 1 ビットへの一般の関数は等分でも定数でもないが，多くの可能な等分関数が存在する．問題は再び f が等分か定数かを（確実に）決定することである．$n = 1$ の場合は以前に考察した問題である．

古典的シナリオにおいて，もし f の 2^{n-1} 個の値を得るために 2^{n-1} 回オラクルへ質問したとして，前の質問の結果に依存するように後の質問をどんな方法を使って作ったとしても，**すべての場合でまだ問題を解くことができない**であろう．ここで，その 2^{n-1} 個の値がすべて同じ値になっていると仮定しよう（関数が実際等分ならば，ありえそうもないことであるが可能性はある）．そのとき，入力の値の選択に関係なく，得られた全体の情報と矛盾なくなお定数関数であり等分関数でもあろう．よって問題に対するどんな古典的な解も 2^{n-1} 回より多く，すなわち少なくとも（n の）指数回数オラクルに質問しなければならない．事実 $2^{n-1} + 1$ 回の質問が常に十分であることを理解することは簡単である．量子的シナリオにおいては，その問題はちょうど **1 回**のオラクルの呼び出しですべての場合に確実に解くことができる．この方法は 1 ビットの場合の直接的な一般化である．

すべての n（入力）量子ビットと 1（出力）量子ビットの並びを標準状態 $|0\rangle$ から始める．入力量子ビットのそれぞれに H を適用する．式 (4.3) で与えられ

ているように，これは最初の n 量子ビットに対しすべての入力の均等な重ね合わせとなる．以前のように，最後の（出力）量子ビットを正確に $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ として準備する．次に，オラクルに結果の $n+1$ 量子ビット状態を与える．これはいま，x が単に B ではなくむしろ B^n 上の領域であるということを除き形式的には (4.9) と同じである．オラクルによる処理の後，最初の n 量子ビットは状態

$$|\xi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in 2^n} (-1)^{f(x)} |x\rangle \tag{4.10}$$

になるであろう（ちなみに，ここで Deutsch のアルゴリズムのオリジナル 1992 年版 [138] では，出力レジスタは状態 $|0\rangle$ に初期化され，オラクルの 2 回の呼び出しが状態 $|\xi_f\rangle$ の生成に必要であったことに注意しよう）．いまもし f が定数関数ならば $|\xi_f\rangle$ はすべてプラスかすべてマイナスの符号をもつちょうどすべての $|x\rangle$ の均等な重ね合わせであり，一方もし f が等分関数ならば $|\xi_f\rangle$ はちょうど $|x\rangle$ の半分がマイナスの符号をもつ均等に重み付けされた重ね合わせである．このように，これら二つの可能性は直交しており，そのため確実に等分と定数関数を区別する $|\xi_f\rangle$ についての相応する測定が存在する．

どのようにこの測定を実行することができるかを明示的に記述する．任意の量子アルゴリズムにおいて，任意の測定を計算の 1 ステップの命令で実行することができると仮定することはできない（ちょうど複雑なユニタリ演算の適用を 1 ステップと仮定できないのと同様である）．任意の測定の複雑さを評価するために利用できる唯一の可能な測定は，計算基底の任意の 1 量子ビットの要素 $|0\rangle$ と $|1\rangle$ の測定であり，これを 1 ステップとして計数すると仮定する．任意の一般的な測定は，測定の固有基底をまず計算基底にユニタリ的に回転させ，続いてそのビットを読むことによりこれら標準的な測定の列に帰着させてもよい．測定の複雑さは，そのときこのユニタリ回転の実行に必要なステップ数に，読まれるために必要な量子ビット数を加えた数により評価する．

今回の場合には，$|\xi_f\rangle$ の定数と等分を区別する測定は単純に以下のように実行してもよい．H は自分自身の逆演算（すなわち $HH = I$）であることと，$|0\rangle|0\rangle \ldots |0\rangle$ の各量子ビットに適用させる H は結果としてすべての $|x\rangle$ の均等な重ね合わせになること（(4.3) 参照）を思い出すと，もし H を再度この均等な重ね合わせの各量子ビットに適用するならば，結果の状態は $|0\rangle|0\rangle \ldots |0\rangle$

になるであろう．よって，(n ステップを要して) $|\xi_f\rangle$ の各量子ビットに H を適用する．もし f が定数であったならば結果の状態は $\pm|0\rangle|0\rangle\ldots|0\rangle$ である．もし f が等分であったならば結果の状態はこれに直交，すなわち $x \neq 00\ldots0$ である $|x\rangle$ の重ね合わせになるであろう．よって測定を完了し，(さらに n ステップを要して) それらがすべて 0 か否かを判断するために n 量子ビットのそれぞれを読む．まとめると，Deutsch の量子アルゴリズムは確実に等分と定数関数を区別するために（オラクルへの 1 回の呼び出しを含めて）$O(n)$ ステップを必要とし，一方任意の古典アルゴリズムは同じタスクを達成するために $O(2^n)$ ステップを必要とする．

Deutsch のアルゴリズムはいわゆる「オラクルを用いた結果」あるいは「相対化の」（オラクルにより相対化された）分離結果である．量子と古典計算の**絶対的な**指数的分離を与えるものではなく，オラクルの内部の仕組みにアクセスすることが禁止されているという事実に関するある付加的な（もっともらしいが証明されていない）計算上の仮定をするときだけこの分離を与える．実質的には，もし f を計算するプログラムが与えられているならば，単に十分な回数そのプログラムを実行することより速く，f が定数か等分かを決定する一般的なプログラムの構文を使う機械的な方法はないと仮定している．もちろん，たとえば定数関数は，定数関数を計算するものとただちに認識される非常に短いプログラムをもつかもしれないが，敵はまた定数関数を計算する非常に複雑に偽装したプログラムを与えるかもしれず，これは構文を読んで理解することが非常に難しいかもしれない．この仮定は非常にもっともらしいものではあるが，プログラムの構文を入力として演算するアルゴリズムを解析することが非常に困難であることと同様に証明されていない！

もし古典と量子計算の間の**絶対的な**指数的分離を証明することができるならば，古典計算量理論のいくつかの基本的な未解決問題は解決されるであろう（たとえば $P \neq PSPACE$ を意味するであろう．これらの用語の定義については [131] を参照）．このように，量子計算が古典計算より指数的により強力であることを形式的に証明することは非常に困難なように思える．

Deutsch のアルゴリズムの別の重要な特徴は，もしアルゴリズムが完全に動作するように要求されていないならば，すなわちもし答えにある（任意に小さな）エラーを許すならば，古典と量子計算の間で示された指数的分離は崩壊する．実際，任意の $\epsilon > 0$ が与えられたとき，(n に無関係な！) **定数**ス

テップ数で実行する古典（確率）アルゴリズムが存在し，f の任意に与えられた選択に対し，確率 $(1-\epsilon)$ で正しい答えを与えるように，等分と定数関数を区別するであろう．このアルゴリズムは単純に以下のように実行する．ある K 個の**ランダム**に選ばれた入力に対し f を評価する．もし答えがすべて同じならば f は定数だと考えられる．さもなくば等分だと考えられる．少し考えてみると「等分」という答えは常に正しいが「定数」という答えは $1/2^K$ より小さなエラー確率で正しいことがわかる．このように，任意に与えられた $\epsilon > 0$ に対し $\frac{1}{2^K} < \epsilon$ を満たす十分大きな K を選ぶ．K は n に無関係であり，K 回の評価はアルゴリズムにおいて定数ステップ数として計数されることに注意しよう．

量子と古典計算の間の指数的分離が発生するのは $\epsilon = 0$ の極限の場合だけである．どんなコンピュータも物理素子であり，その環境から決して完全に分離することはできないので，この極限の状況は実際には非物理的であると言ってもよい．このように，間違って機能するある（一般には非常に小さな）確率が常に存在する．たとえば，メモリビットはどんなときでも宇宙線により反転させられるかもしれない．よって，たとえ結果に小さなエラーが発生するとしても，計算量が量子と古典計算を指数的な量により分離する計算タスクを示すことは非常に興味深いことである．最初のそのような例は Bernstein と Vazirani により与えられた [140]．再帰的な構成を用いて，彼らは量子コンピュータでは多項式時間で解くことができるが，古典コンピュータでは $O(n^{\log n})$ 時間を必要とするオラクルを含む計算タスクについて記述した．それから Simon[141] は，量子コンピュータでは $O(n^2)$ 時間で解くことができるが，古典コンピュータでは完全に指数時間（すなわち $O(2^n)$ 時間）を必要とするより単純なオラクル問題について記述した．この発展の流れの極致は，オラクルの依存をも取り除いた素因数分解のための Shor のアルゴリズム [36] であった．Shor のアルゴリズムは，整数 N の桁数 $(\log N)$ の（3 乗より小さい）多項式のステップ数でかつ任意に指定された $\epsilon > 0$ に対し，確率 $1-\epsilon$ で正しい結果を返す N を素因数分解する方法を与えている．数百年にわたる（Gauss, Legendre, Fermat, その他の著名な数学者による）多大な努力にもかかわらず，この問題に対する**古典**確率多項式時間アルゴリズムは知られていない．Deutsch や Simon のアルゴリズムと異なり，Shor のアルゴリズムはオラクルを含んでいない．しかし，古典多項式時間素因数分解アルゴリズムが存在しないという

証明もまた知られていない（ただそのようなアルゴリズムを構成しようと試みた莫大な量の失敗だけが存在する！）ので，これは古典計算に対する量子計算の絶対的指数的有利さの証明を与えてはいない．

4.2.5 フーリエ変換と周期性

Shor の素因数分解量子アルゴリズムと Simon のアルゴリズムの本質は，与えられた周期関数の周期性を効率的に決定する量子コンピュータの注目すべき能力に依存する．以下の基本例題を用いてそのアイデアを説明する．ある周期 r で周期的であると保証されている関数 $f : \mathcal{Z}_N \to \mathcal{Z}$ を計算するブラックボックスがあると仮定しよう．すなわち

$$\text{すべての } x \text{ に対して} \quad f(x+r) = f(x) \tag{4.11}$$

とする．$\mathcal{Z}_N$ は N を法とする整数の群であり，加算はここでは N を法とすることを思い出そう．また f は，任意の 1 周期当たり同じ値を二度取らないと仮定する．式 (4.11) は r が N を正確に割り切るときだけ成り立つことに注意しよう．

目的は r を決定することである．古典的には（f に関するどんな付加情報もない場合に）r に関する情報を与えるであろう二つの等しい出力結果を期待して，単にブラックボックスに異なる x の値を入力するだけである．一般に高い確率で二つの等しい値を当てるためには $O(N)$ 回のランダムな試行を必要とするであろう．量子効果を用いると単に $O((\log N)^2)$ ステップだけで r を見つけることができ，それはどんな古典アルゴリズムより指数的な高速化を表している．

f のすべての値を計算するために，均等な重ね合わせにより量子並列計算を利用し，状態

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \tag{4.12}$$

を得る．この状態は f の周期性を含んでいるのではあるが，r の情報を抽出する方法はすぐにはわからない！　もし第 2 レジスタの値を測定し，y_0 という値を得るならば，第 1 レジスタの状態は $f(x) = y_0$ となるすべての $|x\rangle$ の均等な重ね合わせに帰着する．もし x_0 がこれを満たす最小の x であり $N = Kr$

であるならば，第 1 レジスタに周期的状態

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle \tag{4.13}$$

を得る．ここで，$0 \leq x_0 \leq r-1$ は，等しい確率で f の任意の値 y_0 に対応し，ランダムに生成されていることに注意する．もし，いまこのレジスタの値を測定するならば，得られた結果からは，r の値に関する情報がまったく得られず，単に一様ランダムに 0 から $N-1$ までの数を生成するだけである！

この問題の解決策は，古典データに対するときと同様，全体のパターンがどのようにシフトするかに関係なくデータ集合の周期パターンを取り出すことができるフーリエ変換を利用することである．N を法とする整数に対する離散フーリエ変換 $\mathcal{F}$ は，要素が

$$\mathcal{F}_{ab} = \frac{1}{\sqrt{N}} e^{2\pi i \frac{ab}{N}} \tag{4.14}$$

である $N \times N$ ユニタリ行列である．もしこのユニタリ変換を上の状態 $|\psi\rangle$ に適用するならば

$$\mathcal{F}|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i \frac{x_0 j}{r}} \left| j\frac{N}{r} \right\rangle \tag{4.15}$$

を得る [144]．ここで注意すべき重要な点は，ランダムなシフト x_0 はもはやケットベクトルのラベルに表れていないということである（図 4.7 参照）．

もしいま，そのラベルを読むならば c という値を得，これは必ず N/r の倍

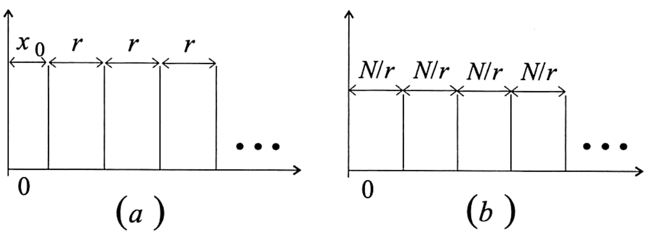


図 4.7　(a) 状態 $|\psi\rangle$ と (b) そのフーリエ変換の周期的振幅のグラフ表現．$\mathcal{F}|\psi\rangle$ により周期性 r は N/r に変換されランダムなシフト x_0 は消去される

数である．すなわち $c = \lambda N/r$ である．よって

$$\frac{c}{N} = \frac{\lambda}{r} \tag{4.16}$$

と書くことができる．ここで c と N は既知の値であり，$0 \leq \lambda \leq r-1$ は（$\mathcal{F}|\psi\rangle$ のすべての振幅は同じ大きさなので）測定により一様ランダムに選ばれている．いま，もしランダムに選ばれた λ が偶然 r と互いに素である（すなわち λ と r が共通の因子をもたない）ならば，c/N を既約分数まで通分することにより r を決定することができる．実際，ランダムに選ばれた λ が r と互いに素である確率はどのくらいか？　素数定理（[142, 143] や [144] の付録 A 参照）に従うと，r 以下の素数の数は大きな r に対し $r/\log r$ となる．このように，ランダムに選ばれた λ が r と互いに素である確率は $1/\log N$ 以上で少なくとも $1/\log r$ である．よってもし上記の手続きを $O(\log N)$ 回繰り返すならば，望むだけ 1 に近づくように任意に指定された確率 $1-\epsilon$ で r を決定することができる．

周期性を決定するどんな既知の古典アルゴリズムより指数的な高速化を達成するために，poly$(\log N)$ の時間で，すなわち N 自身よりむしろ $\log N$ の多項式のステップ数で r を決定する量子アルゴリズムを要求しているということを今まで述べてきた．r を決定するためには $O(\log N)$ 回の繰返しで十分であるが，結論とはまだ大きな隔たりがある．すなわち，用いたフーリエ変換 $\mathcal{F}$ は，サイズ $N \times N$ の，大きな自明でないユニタリ変換であり，poly$(\log N)$ 個の基本演算だけを用いて実現できると**最初から**仮定することはできない．実際，任意の $d \times d$ ユニタリ行列が（演算の任意の万能集合を備えた）量子コンピュータで $O(d^2)$ ステップで実現されるであろう [124, 144]．これはまた $d \times d$ 行列掛ける d 次元列ベクトルの古典計算に必要なステップ数でもある．$\mathcal{F}$ の使用に対し，この $O(N^2)$ の上界は十分ではない．幸運にもフーリエ変換は $O((\log N)^2)$ ステップで実現できる特殊な性質をもっている．これらの性質は古典行列乗算を $O(N^2)$ ステップから $O(N \log N)$ ステップへ減少させる方法を示す高速フーリエ変換 (FFT) の古典理論 [145] に由来する．もし同じアイデアを量子的な設定で実現するならば，局所演算の原理によりステップ数を実現に必要な $O((\log N)^2)$ に減少できることがわかる [134, 144]．ここではこの重要な点を指摘することだけにし，FFT の構成と量子的な設定における多くの技術的詳細については省略する．これらの詳細は [134] に詳しく述べら

れている．式 (4.14) に従い

$$\mathcal{F}|0\rangle = \frac{1}{\sqrt{n}} \sum_{x=0}^{N-1} |x\rangle \tag{4.17}$$

になるので，$\mathcal{F}$ の効率的な実現方法を手に入れることにより，式 (4.12) で $|f\rangle$ を得るために必要な一様に大きな重ね合わせを効率的に生成することができることにも注意しよう．

要約すると，N 入力の，与えられた関数 f の周期性を決定する量子アルゴリズムは，$O(\log N)$ ステップ用いた重ね合わせにより f のすべての値を計算するために量子並列計算を適用することから始める．フーリエ変換は最終状態の周期構造を取り出すために適用される．FFT アルゴリズムの量子的な実装のための局所演算の原理は，フーリエ変換が poly($\log N$) ステップで実現できることを保証している．対応する古典計算は，f のすべての関数値の列ベクトルを計算するための $O(N)$ 回の実行と FFT の実行のための $O(N \log N)$ ステップを必要とする．このように量子アルゴリズムは指数的な高速化を表している．

周期性の概念とフーリエ変換の構成は任意の有限群へ適用するために拡張できるかもしれない．上の議論は N を法とする整数の加群の特殊な場合に属している．一般化した見方はフーリエ変換の仕組みに対し深い洞察力を与える．いまは簡単に，有限アーベル群の場合に制限して，含まれているいくつかの本質的なアイデアを概観する（以下の節とのつながりを失うことなく，望むなら，本節の残りを省略してもよい）．

G を任意の有限アーベル群とする．$f : G \to X$ をその群上の（ある集合 X で値を取る）関数とし

$$K = \{k \in G : \text{すべての } g \in G \text{ に対し } f(k+g) = f(g)\} \tag{4.18}$$

を考えよう（群の演算を加算の表記により表していることに注意しよう）．K は必ず f の安定化部分群 (stabiliser) あるいは対称群と呼ばれる G の部分群である．それは G の群の演算に関し f の周期性を特徴付けている．以前の例では，G は $\mathcal{Z}_N$ で K は r のすべての乗算の巡回群であった．f を計算する素子が与えられたとき，目的は K を決定することである．より正確には，$|G|$ が群のサイズで，一つの入力に対する f の評価が 1 計算ステップとして計数

されるとしたとき，$O(\mathrm{poly}(\log|G|))$ 時間で K を決定することである（単純に f のすべての値を評価し検査することにより $O(\mathrm{poly}(|G|))$ 時間で容易に K を決定できることに注意しよう）．この例では，状態

$$|f\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle \tag{4.19}$$

を構成することから始め，第 2 レジスタを読み込む．f は —— $f(g_1) = f(g_2)$ の必要十分条件が $g_1 - g_2 \in K$ である，すなわち f は各周期内で 1 対 1 対応であるという意味で —— 相応して非退化であると仮定すると，第 2 レジスタが $f(g_0)$ であることに対応し，第 1 レジスタに

$$|\psi(g_0)\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 + k\rangle \tag{4.20}$$

を得る．ただし g_0 はランダムに選ばれている．式 (4.20) は G で K のランダムに選ばれた剰余類に対応するラベルの均等な重ね合わせとなる．いま G は，もし式 (4.20) でラベルを読むならばランダムな剰余類のランダムな要素，すなわち G から任意に等しい確率で選ばれたラベルを見るように，すべての剰余類の互いに素な和集合であり，K に関してまったく情報が得られない．

「G 上のフーリエ変換」の一般的な構成は，（ちょうどこの例のように）ラベルから g_0 を消去する方法を与え，そして最終状態は K に関する直接的な情報を与えるであろう．$\mathcal{H}$ を G の要素によりラベル付けされた基底 $\{|g\rangle : g \in G\}$ をもつヒルベルト空間とする．各群要素 $g_1 \in G$ は

$$\text{すべての } g \text{ に対し } U(g_1)|g\rangle = |g + g_1\rangle \tag{4.21}$$

により定義される $\mathcal{H}$ 上のユニタリ「シフト」演算子 $U(g_1)$ を与える．式 (4.20) の状態は g_0-シフト状態として記述してもよいことに注意しよう．すなわち

$$\sum_{k \in K} |g_0 + k\rangle = U(g_0) \left(\sum_{k \in K} |k\rangle \right) \tag{4.22}$$

となる．基本的な考え方はいま

$$\text{すべての } g_1, g_2 \text{ に対し } U(g_1)|\chi_{g_2}\rangle = e^{i\phi(g_1,g_2)}|\chi_{g_2}\rangle, \tag{4.23}$$

すなわち，$|\chi_g\rangle$ はすべてのシフト演算 $U(g)$ の共通の固有状態であるという意味で**シフト－普遍** (shift-invariant) となる特殊な状態の新しい基底 $\{|\chi_g\rangle : g \in G\}$ を $\mathcal{H}$ に導入することである．$U(g)$ はすべて可換であり，共通の固有状態の基底が存在すると保証していることに注意しよう．よって式 (4.22) に従い，もし新しい基底で $|\psi(g_0)\rangle$ を眺めるならば，そのとき $\sum_{k\in K}|k\rangle$ と $\sum_{k\in K}|g_0+k\rangle$ は部分群 K だけにより決定する同じラベルのパターンを含んでいる．新しい基底でそのラベルを読むことにより，直接 K の構成要素に関する情報が得られる．

G 上のフーリエ変換 $\mathcal{F}$ は，単にシフト－普遍基底を標準基底に戻すユニタリ変換であると定義できる．すなわち

$$\text{すべての } g \text{ に対し } \mathcal{F}|\chi_g\rangle = |g\rangle \tag{4.24}$$

である．よって，新しい基底で $|\psi(g_0)\rangle$ を読むことは，まさに $\mathcal{F}$ を適用し，標準基底で読むことと同じである．

$\mathcal{F}$ の具体的な構成を与えるためには標準基底の成分として記述される状態 $|\chi_g\rangle$ を与えるだけで十分である．群表現論の構成に基づいて，これらの成分を計算する標準的な方法が存在する．ここでは詳細を省略するが，興味のある読者は [134] と [146] を見ていただきたい．群 $\mathcal{Z}_N$ に対し式 (4.14) で与えられたフーリエ変換式

$$|\chi_k\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i\frac{jk}{N}}|j\rangle \tag{4.25}$$

を得る．

上記の群論的枠組みは，周期性の決定のための量子アルゴリズムの応用の一般化と拡張に役立つ．たとえば，Simon の量子アルゴリズム [134, 141, 146, 147] は群 $(\mathcal{Z}_2)^n$，2 を法とする成分ごとの加算を有するすべての n ビット列の群の周期性を決定することである．Simon は次の問題を考察した．n ビット列から n ビット列への関数 f を計算するブラックボックスがあると仮定しよう．またその関数は

$$\text{すべての } n \text{ ビット列 } x \text{ に対し } f(x+\xi) = f(x) \tag{4.26}$$

を満たす，ある決められた n ビット列 ξ が存在するという意味で「2 対 1 対応」であると約束されている．問題は ξ を決定することである．

これがまさに一般化された周期性を決定することであることを理解するために，n ビット列の群 $(\mathcal{Z}_2)^n$ において，すべての要素が $x+x=0$ を満たしていることに注意しよう．すなわち，式 (4.26) は，ちょうど f が周期部分群 $K=\{0,\xi\}$ を有する群上で周期的であることを述べている．よって ξ を決定するために n ビット列の群上でフーリエ変換を構成し，上記の標準的なアルゴリズムを適用する．n ビット列によりラベル付けされた基底をもつ対応するヒルベルト空間 $\mathcal{H}$ は，ちょうど n 量子ビットの行である．群表現論の一般的な構成を用いると，フーリエ変換は n 量子ビットのそれぞれへの（(4.1) の）H の適用であると理解してもよい [134]．量子アルゴリズムは ξ を $O(n^2)$ ステップで決定するが，任意の古典アルゴリズムは f を少なくとも $O(2^n)$ 回評価しなければならない [141]．アルゴリズムの完全な記述は [141, 146, 147] で見いだされる．

フーリエ変換の形式化がこれまで発見された量子アルゴリズムの最も重要な要素であることがわかった．非アーベル群への拡張を含め，そのいくつかの興味深い内容については [148, 149] で見いだされる．

4.2.6 Shor の素因数分解量子アルゴリズム

いままで考案された最も有名な量子アルゴリズムは Shor の効率的な素因数分解アルゴリズムである [36, 144, 146]．整数 N が与えられたとき N を正確に割り切る数 k（1 または N 以外）を決定したいとする．本節では，この問題を相応する周期関数 f の周期性を決定する問題に還元 (reduction) する方法について概観する．そして前節で述べた量子アルゴリズムが N の素因数分解を $\mathrm{poly}(\log N)$ 時間，すなわち N の桁数の多項式で達成するであろう．

まず任意に与えられた N を N の桁数の多項式時間で素因数分解する知られた古典アルゴリズムは存在しないことに注意しよう．たとえば，最もすなおな素因数分解アルゴリズムは，1 から $\sqrt{N}$ まで（任意の合成数 N はこの範囲内で因数をもたなければならないので）の各数で N を割って確かめることである．これは（試行する各因数に対し少なくとも 1 ステップ必要なため）少なくとも $\sqrt{N}$ ステップを必要とし，$\sqrt{N}=2^{\frac{1}{2}\log N}$ は $\log N$ の指数である．実際，現代数学のすべての英知を集めても，最も速い既知の古典素因数分解アルゴリズムは $\exp((\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}})$ のオーダ時間かかっている．

N を素因数分解する問題を周期性の問題に環元するために，数論のいくつ

かの基本的な結果を利用する必要がある．これらは [144] の付録でより詳しく述べられており，完全な解説は [142, 143] のような数論の最も標準的なテキストの中に見いだされる．数 $a < N$ をランダムに選択することから始める．Euclid のアルゴリズムを用い，a と N の最大公約数を poly($\log N$) 時間で計算する．もしこれが 1 より大きければ，N の因数を見いだし終了する！　しかしほとんどの場合，ランダムに選択された a は N と互いに素である（前述）．素数定理はこの確率が大きな N に対し $1/\log N$ を越えることを意味している．もし a が N と互いに素であるならば，そのとき数論の Euler の定理は N で割られたとき余り 1 となる a のべき乗が存在することを保証している．r をそのような最小のべき乗としよう．すなわち

$$a^r \equiv 1 \bmod N \quad \text{ただし} r \text{はそのような最小のべき乗である} \tag{4.27}$$

（もし，a が N と互いに素でないならば，a のべき乗は余り 1 をもたない）．r は N を法とする a の**位数** (order) と呼ばれる．次に，r の情報は N の因数を与えることができることを示す．

r を決定する方法があり（以下参照），さらに r は**偶数**であると仮定しよう．そのとき式 (4.27) を $a^r - 1 \equiv 0 \bmod N$ と書き換えることができ，異なる平方に因数分解できる．すなわち

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \bmod N \tag{4.28}$$

が成り立つ．ここで，$\alpha = a^{r/2} - 1$，$\beta = a^{r/2} + 1$ とする．そのとき N は正確に積 $\alpha\beta$ を割り切る．もし α も β も N の倍数でないならば，N は α の一部と β の一部に分割されなければならない．このように α と β により（また Euclid のアルゴリズムを用いて），N の最大公約数を計算することは N の自明でない因数を生成する．

例として $N = 15$ を取り，それと互いに素である $a = 7$ を選択しよう．15 を法として 7 のべき乗を計算することにより $7^4 \equiv 1 \bmod 15$，すなわち 15 を法として 7 の位数が 4 であることがわかる．このように，15 は正確に積 $(7^{4/2} - 1)(7^{4/2} + 1) = (48)(50)$ を割り切らなければならない．50 と 48 で 15 の最大公約数を計算するとそれぞれ 5 と 3 を与え，実際 15 の自明でない因数である．

この方法は r が偶数でありかつ，$(a^{r/2} \pm 1)$ のどちらも N の正確な倍数でないという条件の下で N の因数を与える．これらの条件が（ランダムに選択された a に対し）しばしば十分に起こりうることを保証するために

定理：N を奇数とし N と互いに素な $a < N$ がランダムに選択されていると仮定する．r を N を法とする a の位数とする．このとき，r が偶数でかつ $a^{r/2} \pm 1$ が正確に N の倍数でない確率は常に 1/2 以上である．□

を与える．この定理の（やや長い）証明は [144] の付録 B に見いだされ，詳細についてはそれが参考になるであろう．

まとめると，この方法はすべての場合において少なくとも半分の確率で N の因数を生成する．この手続きを（N に無関係な定数 K を用い）K 回繰り返すことにより，$1 - \frac{1}{2^K}$ を超える確率で N の素因数分解に成功するので，この成功確率はいくらでも 1 に近づくように増幅できる．

Euclid のアルゴリズムや数の算術操作を適用するすべてのステップは poly$(\log N)$ 時間で実行することができる．唯一残る重要な問題は poly$(\log N)$ 時間で r を決定する方法である．指数関数

$$f(x) = a^x \bmod N \tag{4.29}$$

を考えよう．いま，式 (4.27) は正確に f が周期 r で周期的である．すなわち，$f(x + r) = f(x)$ であるということを述べている．このため，前節で述べた r を見つけるために，周期性を決定するための量子アルゴリズムを利用する．このアルゴリズムを適用するためには，式 (4.29) の x の値の範囲をある q に対し**有限**な領域 $0 \leq x \leq q$ に制限する必要がある．もし q が（未知の）r の正確な倍数でないならば，すなわち，ある $0 < t < r$ に対し $q = Ar + t$ ならば，そのとき起因する関数は正確に周期的ではない —— 最後の t 個の値に対する最後の 1 周期は不完全である．しかし，もし十分大きな q が選ばれるならば，f の十分多くの損なわれていない周期が得られ，そのときただ一つの損なわれた周期は，直感的に期待できるように，r を決定する $q \times q$ フーリエ変換の使用に際し影響を無視できるであろう．実際，もし q がサイズ $O(N^2)$ であるように選ばれるならば，かなり効率的に r を決定できる．この不完全な周期の（連分数の理論を含む）技術的な解析については [36, 144] が参考になるであろう．q はまた，一般に**高速**フーリエ変換の形式化に特によく適する 2 の

べき乗が選ばれる（[134, 145] 参照）．

4.2.7　量子探索と NP

ソートも構造化もされていない N レコードのリストから構成されるデータベースが存在し，高々そのレコードの一つだけが興味対象となる所定の性質を満たしていると仮定しよう．この特別なレコードの位置を探し当てたいと思っている．ある（N に無関係な）定数確率でそのレコードの位置を探し当てるどんな古典的な方法も $O(N)$ ステップを必要とする．実際，初等確率論によると，もし k 個のレコードを調べるならばその特別なレコードを見いだす確率は k/N であることがわかる．この確率は k が少なくとも N のオーダでないならば N の増加に伴って 0 に近づいていく．Grover の量子探索アルゴリズム [120, 150] はこの問題をほんの $O(\sqrt{N})$ ステップで解決する．以前議論された量子アルゴリズムで示された非常に大きな指数的な高速化と対比すると，この問題では量子効果は平方根の高速化を与える．Grover のアルゴリズムでは，ちょうど入力値の重ね合わせにより関数を評価する今までのアルゴリズムと同様，重ね合わせにより種々のレコードを調べる能力を必要とする．

データベースの非構造化の仮定は結果に対し非常に重要である．たとえば，もしデータベースが昇順に**ソートされた** N 個のランダムな数から構成されていたならば，そのとき，それらの数の任意に与えられた一つを探し当てるために古典的に（標準的な 2 分割法を用いて）ほんの $O(\log N)$ ステップを必要とするだけである．同様に，データベースの前もって知りうるどんな構造も探索時間を減少させるために活用できるかもしれない．非構造化の仮定は，以前利用したアクセスできない内部構造をもつオラクル（またはブラックボックス）に類似している．実際，データベース探索問題は以下のようにオラクルを用いてより正確に書き直せる．N 入力の，出力値が 0 または 1 となる関数を計算するブラックボックスが与えられている．さらに，正確に一つの入力値 x_0 に対し $f(x) = 1$ （f の他のすべての値は 0）であると保証されている．問題は x_0 を見つけることである．

いま x_0 を $O(\sqrt{N})$ ステップで見つける Grover の量子探索アルゴリズムの概略を述べる（すでに述べたアルゴリズムの特徴に注意すると，もし最初に読む際には，話の流れを本質的に損ねないため，以下の技術的な詳細について省略してもよい）．Deutsch のアルゴリズムや量子並列計算の議論のよう

に，オラクルは $|x\rangle|j\rangle$ を $|x\rangle|j \oplus f(x)\rangle$ に変換するユニタリ変換 U_f として与えられていると仮定できる．ここで $1 \leq x \leq N$，$j=0$ または 1，$\oplus$ は 2 を法とする加算である．また f は n ビットから 1 ビットへの関数なので，$N=2^n$ すなわち N が 2 のべき乗である場合に制限すると都合がよい．$\mathcal{B}^n$ をすべての n ビット列 x によりラベル付けされた標準基底 $\{|x\rangle\}$ をもつ n 量子ビットのヒルベルト空間（すなわち，入力レジスタ）とする．Grover のアルゴリズムの原型は，$\mathcal{B}^n$ 上でそれぞれ作用する二つのユニタリ演算 I_{x_0} と D に基づいている．I_{x_0} は $|x_0\rangle$ の振幅を単に反転させる演算である．すなわち

$$I_{x_0}|x\rangle = \begin{cases} |x\rangle & x \neq x_0 \text{ のとき} \\ -|x\rangle & x = x_0 \text{ のとき} \end{cases} \tag{4.30}$$

これはちょうど Deutsch のアルゴリズムと同様に，その出力レジスタ（最後の $n+1$ 量子ビットめ）を $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ にまず設定することにより U_f から容易に構成できる．U_f の動作はそのとき出力レジスタを状態 $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ に保ちながら入力レジスタに I_{x_0} を実行する（図 4.8 参照）．

演算子 D は以下のように定義できる．H_n を n 量子ビットのそれぞれへの H（式 (4.1) 参照）の適用とし，I_0 を $x=00\ldots0$ のときの演算子 I_{x_0} とする．このとき D は

$$D = -H_n I_0 H_n \tag{4.31}$$

により定義できる．D の行列要素を直接計算する [120, 150] と（ここで $N=2^n$ であることを思い出すと），すべての非対角要素が $\frac{2}{N}$ で，すべての対角要素が $-1+\frac{2}{N}$ であることがわかる．よって

$$D|x\rangle = -|x\rangle + \frac{2}{N}\sum_y |y\rangle \tag{4.32}$$

となる．D は「平均を基準とした反転 (inversion about the mean)」という単純な幾何学的解釈をもっている．任意の状態 $|\psi\rangle = \sum a_x|x\rangle$ に対し $D|\psi\rangle = \sum a'_x|x\rangle$ とし，$\bar{a} = \frac{1}{N}\sum a_x$ を状態 $|\psi\rangle$ に対する平均の振幅を表すものとする．式 (4.32) を用いると

$$a'_x = -a_x + \frac{2}{N}\sum_y a_y = \bar{a} - (a_x - \bar{a}) \tag{4.33}$$

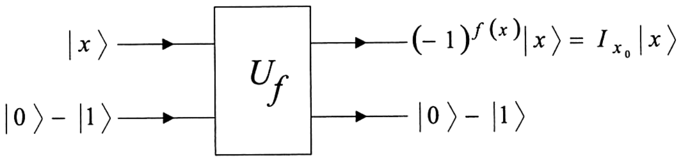


図 **4.8**　U_f を用いた I_{x_0} の構成法．ここで f は x_0 に印を付けるオラクルである

となる．$\Delta a_x = a_x - \bar{a}$ と書くと振幅の値がちょうど平均 $\bar{a}$ で反転しているように $a_x = \bar{a} + \Delta a_x$ と $a'_x = \bar{a} - \Delta a_x$ になる．

Grover のアルゴリズムを実行するために，たとえば，$|0\ldots0\rangle$ に H_n を適用することにより準備できる均等な重ね合わせ $|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum|x\rangle$ から始める．この状態は均等な重ね合わせによりデータベースのすべての場所を調べることに対応する．意図することは $x = x_0$ に振幅を集めるために $|\psi_0\rangle$ を更新することである．アルゴリズムは演算子 DI_{x_0} を繰り返し適用し，状態 $|\psi_k\rangle$ の列を得ることにより構成する．

$$\begin{aligned} |\psi_0\rangle &= \tfrac{1}{\sqrt{N}}\sum|x\rangle \\ |\psi_{k+1}\rangle &= DI_{x_0}|\psi_k\rangle \end{aligned} \tag{4.34}$$

D と I_{x_0} に対する式を用いると，$x \neq x_0$ となるすべての $|x\rangle$ の振幅は各 $|\psi_k\rangle$ が

$$|\psi_k\rangle = \alpha_k \sum_{x \neq x_0} |x\rangle + \beta_k|x_0\rangle \tag{4.35}$$

の形を採るように互いに等しいことが容易に確かめられる．ここで α_k と β_k は実数である．D と I_{x_0} の行列要素を用いると以下の漸化式を導くことができる．

$$\begin{aligned} \alpha_0 = \beta_0 &= \tfrac{1}{\sqrt{N}} \\ \alpha_{k+1} &= (1 - \tfrac{2}{N})\alpha_k - \tfrac{2}{N}\beta_k \\ \beta_{k+1} &= (1 - \tfrac{2}{N})\beta_k + (N-1)\tfrac{2}{N}\alpha_k \end{aligned} \tag{4.36}$$

正規化は

$$\beta_k^2 + (N-1)\alpha_k^2 = 1 \tag{4.37}$$

であり，$\alpha_k = \frac{1}{\sqrt{N-1}}\cos\theta_k$，$\beta_k = \sin\theta_k$ と書けることを連想させる．すなわ

ち，式 (4.36) の漸化式が

$$\alpha_k = \frac{1}{\sqrt{N-1}} \cos(2k+1)\theta, \quad \beta_k = \sin(2k+1)\theta \tag{4.38}$$

を満足することは簡単に確かめられる [151]．ここで θ は $\sin\theta = \frac{1}{\sqrt{N}}$ により与えられる角度である．

このように，β_k は繰返し数 k とともに正弦関数的に変化する．もし $(2k+1)\theta = \pi/2$ ならば，すなわち，もし $k = \frac{\pi - 2\theta}{4\theta}$ ならば $\beta_k = 1$ となる．大きな N に対し $\sin\theta = \frac{1}{\sqrt{N}} \approx \theta$ であり，$\sqrt{N}$ のオーダである $k = \frac{\pi}{4}\sqrt{N} - \frac{1}{2}$ になる．このように，もしこの k の値に最も近い整数により与えられるステップ数その処理を繰り返すならば，そのとき標準基底で最終状態を読むことにより（N に独立な）高い確率で x_0 が得られるであろう（複雑な確率のより高度な解析については [151] を参照）．これでこのアルゴリズムは完成する．

Grover の最初の研究結果ののち，上記のアルゴリズムの基本的な考え方が，N 個の与えられた数のデータベースの平均やメジアンの評価 [152]，またデータベース内で 1 項目以上印の付いた項目が存在する場合の解析 [151, 153] など，さまざまなより進んだ応用問題へ拡張されてきている．Grover のアルゴリズムと Shor のアルゴリズムを巧妙に組み合わせることにより，Brassard, Hoyer, Tapp は（場所を探し当てるよりむしろ）そのような印の付いた項目の**個数**をも評価できることを示した [153]．基礎となる考え方は，おおまかに言うと，印を付けられた項目の個数から定まる周期により上記の振幅 α_k と β_k が周期的に変化するという点である．周期性はそのとき，以前の節で述べられたように，量子フーリエ変換を用いて評価される．一見すると多少驚くが，D の定義のユニタリ演算 H_n はほとんど任意のユニタリ演算子 U に置き換えることができ，変更した D を用いたアルゴリズムもなお $O(\sqrt{N})$ ステップで x_0 を見いだすことができることも示されている [151, 153, 154]．

Grover のアルゴリズムは可能な限り指数的に大きな空間を探索する手段を与える．一般に，指数的な探索は数学や計算機科学の多くの分野で基本的な重要性をもっている．特に興味深いものは任意の候補となる項目に対し,（探索しようと）要求された性質が満たされているかを**多項式**時間で確かめることができる状況である．すなわち，直感的にはその性質自身を確かめることは「計算上単純」であるが，指数的に多くの候補の中に一つ存在するか否かを決定する必要がある，という状況である．一つの例証として，頂点と選ば

れた頂点に接続する辺の集合として記述されるグラフが与えられていると仮定しよう．n 頂点のグラフは，行列の位置 ij の要素が 1 となる必要十分条件が頂点 i を頂点 j に接続する辺が存在する，としたときの 0 と 1 の $n \times n$ 行列として符号化してもよい．グラフから各頂点を一度，そしてただ一度だけ訪問する閉路を見つけることができるか否かを決定したい．これは多くの重要な応用をもち，ハミルトン閉路問題と言われる．いまグラフが与えられたとき，一般に指数的に可能な数の閉路（すなわち，グラフの記述のサイズの関数として指数的に多くの閉路）が存在するが，与えられた任意の閉路に対し要求された条件を満たすか否かを多項式時間でチェックする（すなわち，ちょうど閉路を廻り各頂点を正確に一度だけ訪れるか否かを確かめる）ことは容易である．計算の理論では，この種のすべての決定問題のクラスは NP と呼ばれる（広範な議論については [131, 132] 参照）．NP の性質としては，直感的には，満たしている事例を見つけることは「困難」であるが，候補となる事例が与えられると，その性質を満たしているか否かをチェックすることは「容易」である．

重要な数学的かつ実用的な興味の対象となる多くの計算問題は NP に属している（長くかつさまざまな実例のリストについては [132] を参照）．たぶん古典計算量理論の最も有名な未解決問題，いわゆる $P \neq NP$ 問題は NP 内のすべての計算タスクが実際多項式時間で解くことができるか否かを確立することである．ここで動機付けとなる考え方は，もしある性質を確かめることが「計算上単純」であるならば与えられた構造の中にそれが存在するか否かの質問もたぶんまた多項式時間で決定することができたほうがよいということである．ここでは指数的に多くの候補のなかの全数探索（それは確かに指数時間必要とするが）を考えているのではなく，指数的に多くの可能性を生成した構造それ自身のある有効な解析を考えていることに注意しよう．たとえばハミルトン閉路問題で，ちょうど順番に各閉路を愚鈍にテストするかわりに，ハミルトン閉路をもつか否かを確かめるためにグラフそれ自身の記述を調べる方法があるだろうか？

NP のいくつかの問題 [132] の複雑かつ広範囲な領域を考えると多項式時間で解くことができそうにないように思えるが，この問題は多くの注意が払われているにもかかわらず，未だに証明されていない！　問題の特別な構造についてのいくつかの特殊な数学的性質に頼る必要があることに注意しよう．

たとえばハミルトン閉路問題では，その解はグラフ理論のある深遠な新しい定理を創り出すことと等価であろう．

Grover の探索アルゴリズムの話に戻ろう．ここでデータベースは量子的方法でも（上記の注意と対比して）なお**構造化されてない**ことを要求されていたが，直接的な全数古典探索に対し平方根の高速化を達成した．この高速化は任意の NP 問題の全盲探索に応用することができる．いま非常に重要な疑問は次のことである．指数的に多くの候補をもつ**構造化されてない**領域の探索は，量子効果を用い，あるより巧妙な方法で**さらに**高速化することができるか？　実際，指数的に大きな重ね合わせを線形時間で生成することができ (4.3)，これらの大きな重ね合わせは，そのときたった1回の質問だけで指数的に多くの関数の値を検査するために用いることができることを見てきた（式 (4.4) 参照）．量子計算の初期には，この効果が NP 問題を多項式時間で解く量子的方法の可能性へ向けて，可能な限り指数的に大きな構造化されてない領域を多項式時間で探索する方法を導くと期待された．たとえばグラフが与えられているとき，重ね合わせによりすべての可能な閉路を調べることはできるが，高い確率でハミルトン閉路が存在するか否かを決定するためにこの効果を利用することができるだろうか？　この期待は，Grover のアルゴリズムで示された平方根の高速化を超えて非構造化探索を高速化することができる量子的な過程はないことを厳密に証明した Bennett，Bernstein，Brassard，Vazirani[155] により打ち砕かれた．大雑把に言うと，直感的なアイデアは以下の通りである．1 回の質問で重ね合わせにより指数的に多くの候補を確かめることはできるのだが，重ね合わせによる指数的な要素数のため，要求される性質の記録は一般に単に指数的に小さな振幅としてのみ現れる．よって任意の定数程度の確率でその性質を記録するためには，その処理は指数回繰り返されなければならない．

このように量子計算の状況において，ちょうど古典計算と同様，もし多項式時間で NP 問題を解きたいならば，ある知的な方法で問題の構造を活用することが本質的であろう．たとえば，Simon や Shor のアルゴリズムでの指数的な高速化はフーリエ解析の技術を経て周期性の理論の特殊な数学的性質を利用している．不運にも，クラス NP すべてと多項式時間計算可能性との関係に関する重要な問題は，一見したところでは古典計算量理論の状況より量子的状況で解きやすくはないことがわかる．

4.3　捕捉されたイオンを用いた量子ゲートと量子計算

(*J.I. Cirac, P. Zoller, J.F. Poyatos*)

4.3.1　はじめに

量子計算が驚くべき能力を提供できるということは，本章のいままでの議論から明らかである．問題は，量子論理ゲートのような，量子計算の基本素子を実現することができるか，そしてもしできるならば，どのようにしてかつどのような種類の物理系か，ということである．一般的な議論の代わりに一つの特殊な例に焦点を当てよう．捕捉されたイオン (trapped ions) を用いた量子コンピュータの実現に関するいくつかの詳細な提案について述べよう [156, 157]．この枠組みでは，各量子ビットはイオンの基底電子状態 ($|0\rangle$) と励起（準安定）状態 ($|1\rangle$) の重ね合わせにより実現できる（図 4.9 参照）．レーザ光と相互作用しリニアトラップの中で運動するイオンの集まりが量子コンピュータを実現する真の物理系となることが示されるであろう．

4.3.2　捕捉されたイオンを用いた量子ゲート

N 個のイオンがリニアポールトラップの中に閉じ込められている状況を考えよう．それは静電場と交流電場（第 5 章参照）の組み合わせによりイオンを捕捉し閉じ込めることができるものである．イオンは基本的に 1 次元，軸方向にのみ移動する．なぜならば，この方向に捕捉ポテンシャルがやや弱く，いくつかのレーザ場と相互作用するからである（図 4.10）．

イオンの動作の組み合わせは数種類の光学的波長のイオン間を分離するために用いられる他の一般的などんな相互作用よりはるかに強いクーロン斥力により与えられる．

捕捉されたイオン系の初期の優位さの一つは，量子状態を準備し操作するために要求される技術の多くがすでに高精度分光や周波数標準の目的のために開発されてきているということである．このように，電子状態のラビフリッピングや測定は両方とも十分に開発された道具であり，計算の基本部分を構成するであろう．ラビフリッピング，すなわち内部状態間のコヒーレントな遷移は，一定時間レーザパルスを照射することにより実行できる（たとえば，π パルスは励起状態から基底状態，あるいはその逆へ完全に個体数を変える）が，内部量子状態の測定はいわゆる量子飛躍技術を用いて実行できる．倍共

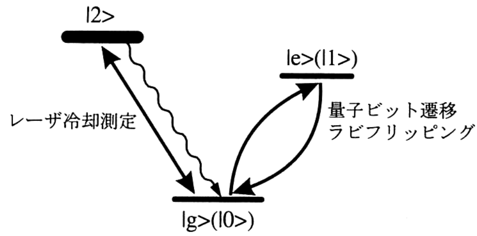


図 4.9 単一イオンの内部準位の倍共鳴構造．弱い遷移に伴うこれらの準位は量子ビット $(|0\rangle, |1\rangle)$ として振る舞う．一方，双極子により許容された遷移により $|0\rangle$ 状態と結合している第 3 準位，$|2\rangle$ は，量子飛躍技術により，冷却と検出に用いられる

鳴状態，ここでは一つの遷移は強く共鳴し他の一つは弱く共鳴している状態を考えるとき，量子ビットとして選ばれた選択準位の状態を測定することが可能である．これはそれぞれ各遷移をさせる二つのレーザビームを用いることにより実行できる．量子ビットの状態は,（双極を許容する）強い遷移から自発的に放射される光の有無により測定されるであろう．図 4.9 を参照せよ．この検出の枠組みはほとんど単位を構成する能力であると証明されている．一方，イオンの動作をこれらの平衡位置のまわりの小さな振動へ帰着するレーザ冷却技術もまた利用できるであろう．つまり，レーザ冷却は放射圧力，すべての光ビームに伴う運動量の効率的な利用に基づいている．そのような運動量は，巨視的な尺度では無視されるものであるが，それにもかかわらず原子の速度をかなり減衰させるのに十分大きな力を発揮することができる（この力は $10^4 g$ ぐらいの大きさにできる．ただし g は重力加速度である）．そのような力を用いる効率的な方法はドップラー効果による．すなわち，この方法により，レーザビームの伝播の方向と反対に動くイオンはかなり運動が減衰する力を受けるであろう．

イオンは単に平衡位置のまわりで非常に小さな振動を受けるように全 3 次元方向に冷却されるレーザであると仮定しよう．この場合，イオンの動作は，通常の方法で独立に量子化された非連結な調和振動子の集まりと等価である標準モードにより記述できる．必要なこととして，各モードに対しいわゆるラム－ディッケ領域を満たすことが要求され，それは物理的に適用される放

射の波長よりはるかに小さな領域にイオンが閉じ込められていることを意味する．

量子コンピュータを実現する作業は 1 量子ビットと 2 量子ビットのゲートを実現する方法を見つけることと等価である．なすべきことは量子ビットの内部状態間でラビフリッピングを誘導することのみなので，1 量子ビットゲートは単純であろう．すでに述べたように，これは捕捉されたイオンの場合によく知られた技術である．2 量子ビットゲートは実現することがより困難である．主要な問題は量子力学的に，すなわちコヒーレントな重ね合わせを維持しながら，2 量子ビットを結合する方法を見つけることである．これを行うために，イオン列に伴う外部自由度を考えよう．特に，最小量子化モード，すべてのイオンがまるで結合した一つの質量であるかのように運動を記述する質量中心 (center-of-mass, CM) 運動を利用する．挑戦すべきことは，内部量子ビットからの情報を**量子ワイヤ**へ移す CM 運動である．一度これが達成されるならば，この方法により 2 量子ビット間でコヒーレントな相互作用を実現しながら，**量子ワイヤ**からの情報を他の選択された量子ビットへ移すことが可能となるであろう．

4.3.3　レーザ光と相互作用する N 冷却イオン

本項は，イオンとレーザのシステムを記述する方法と量子計算を実現する能力についてかなり詳細に示しており，少し専門的である．与えられたイオン i と定常レーザ波の相互作用を考えよう（進行波は同じ方法で研究することができる）．この状況を記述するハミルトニアンは，レーザ周波数により回転する枠組みで，$H = H_{\rm ex} + H_{\rm int} + H_{\rm las}$ により与えられる．ここで $(\hbar = 1)$

$$H_{\rm ex} = \sum_{k=1}^{N} \nu_k a_k^\dagger a_k$$

$$H_{\rm int}^i = -\frac{\delta_i}{2}\sigma_z^i$$

$$H_{\rm las}^i = \frac{\Omega_i}{2}\sin(k_L r_i + \phi_i)(\sigma_i^+ + \sigma_i^-) \tag{4.39}$$

である．ただし，$\delta_i = \omega_L^i - \omega_0^i$ はレーザデチューニング（ω_L^i はレーザの周波数であり ω_0^i は量子ビットの遷移に伴う周波数），ν_k はさまざまな標準モード

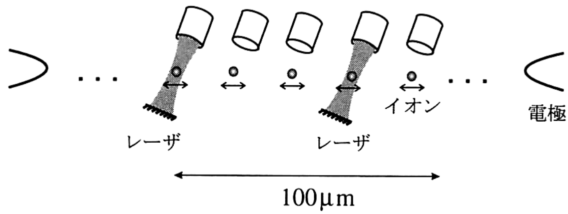


図 4.10 レーザ光と相互作用するリニアトラップ内の N 個のイオン．イオンの動作は量子ビット内のデータバスとして用いられる

の周波数，Ω_i はラビ周波数 [1]（適用されるレーザ場により誘発されるコヒーレントな発展の割合），k_L はレーザ波ベクトル（レーザビームは普通，捕捉軸に斜めの方向に適用され，この場合 k_L は $k_\theta = k_L \cos(\theta)$ により与えられる．図 4.10 参照），ϕ_i は定常波に関するイオンの状況を記述する位相，r_i は（一般に標準モードの線形組み合わせとして表される）イオンの位置である．加えて，2 準位（スピン 1/2）原子に伴うパウリ演算子と量子調和振動子に伴う生成（消滅）演算子を用いている．

レーザビームがそれらのイオンの一つに作用するとき，それは（内部の）基底準位と励起準位の間で遷移を誘発し，集団標準モードの状態を変えることができる．しかし，ラム－ディッケ領域内で，また十分弱いレーザ強度を考えると，CM 運動のみが変更されるであろう．これらの制限下においてレーザとの相互作用は

$$
\begin{aligned}
H^i_{\mathrm{las}} &\approx H^i_a + H^i_b \\
&= \frac{\Omega^a_i}{2}(\sigma^+_i + \sigma^-_i) + \frac{\Omega^b_i}{2}\frac{\eta_{\mathrm{cm}}}{\sqrt{N}}(a_{\mathrm{cm}}\sigma^+_i + a^\dagger_{\mathrm{cm}}\sigma^-_i)
\end{aligned}
\tag{4.40}
$$

の形をとるであろう．ただし η_{cm} は ν_z，CM モードの周波数に一致する軸方向の抑制周波数に伴うラム－ディッケ・パラメータである．上記のハミルトニアンは $\Omega^a_1 \neq 0(\delta_a = 0)$ か $\Omega^b_1 \neq 0(\delta_b \approx -\nu_1)$ のときだけ有効である．これはイオンの運動を変更する (b) か変更しない (a) の二つの利用可能な相互作用を見いだすことを意味している．

いま，上で述べた相互作用を利用し，1 または 2 量子ビット間の量子ゲー

[1] この名前は，原子や分子の内部準位間で遷移を誘発するために発振磁場を用いる最初のアイデアを開発した I. I. Rabi に由来する．

トを実現する方法を示す．単一量子ビット量子ゲートは実現しやすい．なぜなら，運動状態を変更することなく，単一イオンの個々の回転だけでよいからである．それらは定常波レーザビームの波腹に置かれたイオンにより内部遷移周波数 ($\delta_i = 0$) と共鳴するレーザを用いて実現できる．この場合の発展は，以下の回転

$$
\begin{aligned}
|g\rangle_i &\to \cos(k_L\pi/2)|g\rangle_i - ie^{i\phi}\sin(k_L\pi/2)|e\rangle_i \\
|e\rangle_i &\to \cos(k_L\pi/2)|e\rangle_i - ie^{-i\phi}\sin(k_L\pi/2)|g\rangle_i
\end{aligned}
$$

を誘発するハミルトニアン H_a^i により与えられることがわかっている．

一方，2 量子ビットゲートは実現することがより困難であろう．まず $\delta_i = -\nu_z$ として選ばれたレーザ周波数を考えよう．すなわち，それは CM モード，そして定常波レーザビームの波節に置かれたイオンのみに励起する．そのレーザとの相互作用は上記のハミルトニアン H_b^i により与えられる．一定時間 $t = k\pi/(\Omega_i^b\eta_z/\sqrt{N})$ （$k\pi$ パルス）の間レーザを適用すると状態は以下の

$$
\begin{aligned}
|g\rangle_i|1\rangle &\to \cos(k_L\pi/2)|g\rangle_i|1\rangle - ie^{i\phi}\sin(k_L\pi/2)|e'\rangle_i|0\rangle \\
|e'\rangle_i|0\rangle &\to \cos(k_L\pi/2)|e'\rangle_i|0\rangle - ie^{-i\phi}\sin(k_L\pi/2)|g\rangle_i|1\rangle \\
|g\rangle|0\rangle &\to |g\rangle|0\rangle
\end{aligned}
\tag{4.41}
$$

のように発展する．ただし $|0\rangle(|1\rangle)$ は 0(1) フォノンの CM モードを表し，ϕ はレーザの位相，$|e'\rangle$ は（$|e\rangle$ と表される）量子ビットの状態 $|1\rangle$ とみなされるか，選択的に励起された補助電子状態である（この選択励起はいくつかの偏光か周波数により実現できる．実験的には周波数は偏光より制御しやすいように思える）．2 量子ビット論理量子ゲートは以下のように実現できる．(i) 第 1 イオンに位置付けられた π パルスを用い，第 1 イオンの内部状態と CM モードの運動状態を入れ替える．(ii) 補助準位 $|e'\rangle_i$ を用い，第 2 イオンに対し 2π パルスにより条件付符号の交換を行う．(iii)π パルスにより CM モードの量子状態と第 1 イオンの内部状態を元に戻す．完全な発展は

$$
\begin{array}{lllllll}
|g\rangle_1|g\rangle_2|0\rangle & \xrightarrow{(i)} & |g\rangle_1|g\rangle_2|0\rangle & \xrightarrow{(ii)} & |g\rangle_1|g\rangle_2|0\rangle & \xrightarrow{(iii)} & |g\rangle_1|g\rangle_2|0\rangle \\
|g\rangle_1|e\rangle_2|0\rangle & \longrightarrow & |g\rangle_1|e\rangle_2|0\rangle & \longrightarrow & |g\rangle_1|e\rangle_2|0\rangle & \longrightarrow & |g\rangle_1|e\rangle_2|0\rangle \\
|e\rangle_1|g\rangle_2|0\rangle & \longrightarrow & -i|g\rangle_1|g\rangle_2|1\rangle & \longrightarrow & i|g\rangle_1|g\rangle_2|1\rangle & \longrightarrow & |e\rangle_1|g\rangle_2|0\rangle \\
|e\rangle_1|e\rangle_2|0\rangle & \longrightarrow & -i|g\rangle_1|e\rangle_2|1\rangle & \longrightarrow & -i|g\rangle_1|e\rangle_2|1\rangle & \longrightarrow & -|e\rangle_1|e\rangle_2|0\rangle
\end{array}
\tag{4.42}
$$

により与えられる．この方法により，相互作用の正味の効果は両方のイオンが（内部）励起状態であるときのみ符号を変える．ゲートの前後でCMモードは真空状態 $|0\rangle$ であることに注意しよう．結局，これらの演算を用いてすべてのイオンの集まりで n 量子ビットを操作する論理ゲートを実現することができる．

4.3.4 非零度での量子ゲート

前節でリニアトラップ内のイオンの集まりから構成される系がどのように実験室における量子計算の真の実現の有望な候補でありそうかということを見てきた．レーザ冷却され捕捉されたイオンを用いた計算のために基本的に必要なことは，ハミルトニアン演算の正確な制御，集団フォノンモードのための純粋な初期状態を準備するために，振動する基底状態までイオンを高次にデコヒーレンスし冷却することであるように思える．第7章で議論されるエラー訂正とデコヒーレンスの内容に深くかかわってくるので，最初の二つの問題にはかかわらないが，いま零度の極限まで冷却する制約がどのように克服されるかを示そう．

リニアトラップ内の二つのイオンの場合を考えてみよう．新しいアイデアは，レーザ誘発光子の吸収または放射に依存してイオンの運動波束の一つを右または左に移動させることである．その後，捕捉内の第2イオンの位置は第1イオンに基づく動力学に従う．この方法により，第2イオンの内部状態を位置に依存して変化させることができる．これは結果として計算に不可欠な論理量子ゲートになる．つまり，第2イオンの最終内部状態は第1イオンの初期内部状態に依存している．

ある意味，原子干渉計構成法からアイデアを借りてきている．そこでは原子の波束は普通，ある種の光学干渉解析のように，それぞれ異なる動力学に従いながら，さまざまな部分に分割され，処理の終わりに包括的な情報を得るために結合させられる．

特に2量子ビットゲートの演算がどのように実現できるかを示す．まず，レーザビームにより，イオン1は光子の吸収（放射）によりその内部状態に依存して左または右にはじき出される．それから，他のイオンはイオン1の内部状態に従うクーロン斥力によりはじき出される．対応する波束は（イオン1に対し右，左等を表す $1_R, 1_L, \ldots$ と記述される），制御イオンの内部状態

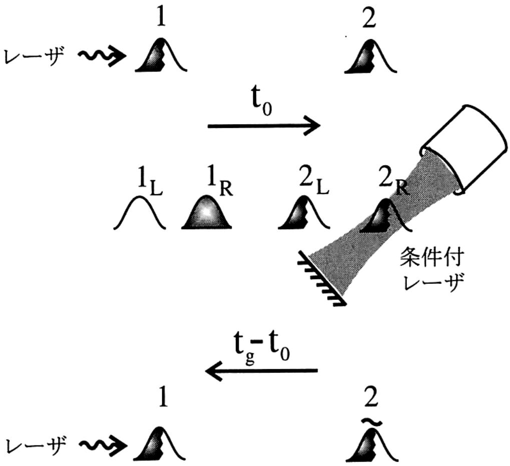


図 4.11　非零度下での 2 量子ビットゲートのためのレーザと波束の構成．ゲートの実現の後，標的量子ビット（イオン 2）の内部状態は，制御量子ビット（イオン 1）の内部状態に依存して，(ティルダ (˜) により表された) 変化するであろう．すなわち，活性化された光子の吸収または放射により右または左にはじき出されるであろう．ここで，波束の暗く（明るく）塗られた個所は内部励起（基底）状態を表す．詳細は本文を参照

としてエンタングルされている二つの可能な空間波束に発展する．これらの波束の空間的分割が（与えられた時刻 t_0 で）それほど大きくないならば，その空間上の位置に依存しながら，すなわち制御イオン（イオン 1）の状態に依存しながら，標的イオン，イオン 2 の内部状態を操作することができ，量子ビット上でのゲート操作を実現することができる．やがて，これらの原子の波束は捕捉内で振動し，適当な一連のレーザパルスにより二つのイオン間で遷移したこの運動量は，(時刻 t_g で）最初の運動状態に回復させることができる．図 4.11 を参照せよ．よってイオンの運動状態は，それが混合状態か純粋状態かに関係なく，すなわち温度に無関係に，ゲートの前後で内部の原子状態から分離するであろう．

要約すると，本節では量子計算を実現するための有望な系を導入した．二つの完全に異なる状況，すなわち零度と非零度を考慮したイオンを用いる条件付き動力学を提案した．零度下の方式に関する原理の証明は小型イオント

ラップ量子計算を構築することが非常に近い将来に実現するであろうことを指摘するNISTのD. Winelandのグループによりすでに報告されていた[158].
次章では量子論理ゲートの種々の実験的実現の状況が述べられるであろう.

第5章

量子計算の実現に向けた最先端の実験

5.1 はじめに

量子計算の基本的な理論上の考えは前の章で説明した．けれども実際に量子コンピュータを作り上げるのはどれぐらい実行可能なのだろうか．一つの量子ゲートでさえも，環境の揺動から高度に隔離され，かつ，互いに強く相互作用している二つの量子系を必要とする．このことをよくわきまえれば，とても楽観的ではいられないだろう．この章で示されるいくつかの実験技術とそれらにより得られた結果は，高度に制御されかつ互いに強く相互作用している，少数の量子系を想定しうることを示唆する．しかしながら，実用的な量子計算にまで拡大することが可能であるかどうかはまだよくわかっていない．

三つの実験方法が，小規模の量子論理操作のために適切な実験的な状態を実現することに成功している．それらは，共振器量子電気力学（キャビティQED），イオントラップ，および核磁気共鳴 (NMR) に基づいている．最初の二つの方法は，結合された量子力学的な系のもっとも単純なものの一つである，一つの量子振動子と結合した単一の 2 準位系を実現する．これらに共通する特徴を強調するために，5.2 節では共振器量子電気力学の実験と並行して，それと対応するイオントラップによる実験を紹介する．

共振器量子電気力学の実験は，特にこれまで量子力学の基本的な特徴を実証することに成功してきた．たとえば，5.2.3 項で紹介する量子ラビ振動や，

5.2.4 項で示すシュレーディンガーの猫状態と量子デコヒーレンスなどである．これらの実験は，美しい方法で基本的な量子論理操作を実行してみせる．しかし，これらの技術を用いて，多数回の論理操作を行うことは非常に困難に思われる．

この規模増大の問題の点から見ると，イオントラップによる実験は将来性があるように思われる．というのは，(多数の) イオンを，直線上のトラップ (捕獲器) に冷却して並べることが可能だからだ．この一列のイオンは，量子ビット (qubit) からなるレジスタと見なすことができる．その中で，(単一イオンに蓄えられた) 量子ビットは，しっかり焦点を合わせたレーザ光線によって個々に制御が可能だ．5.2.5 項から 5.2.12 項において，一つひとつのイオンの電子準位を用いて量子論理を実行できることを見る．また，5.3 節において，イオン列を用いた量子計算の実現に向けた実験の一般的な概説を行う．

量子計算に向け研究されている 3 番めの方法は，核磁気共鳴 (NMR) に基づくものである．この方法は，すでに単純な量子論理操作の小規模の組み合わせの実行に成功している．NMR は，磁場中での原子核の ゼーマン副準位間の遷移を伴う．分子中の原子核からの NMR 信号の周波数は，その原子核周辺の化学的な環境に明確に依存する．これを用いると，単一分子中の異なる核スピンを扱うことが可能になる．これらのスピンは量子ビットの役割をはたし，そして分子内の強いスピン結合相互作用を通じて互いに相互作用する．これらによって，量子計算の基本的な要素が実現できる．5.4 節で，NMR 量子計算の原理を述べる．

量子論理を行うことへのいっそう投機的な道のりは，固体デバイスに基づくものである．このようなデバイスの製作において突破口を開くことは極めて重要であろうけれども，この分野の研究は，まだこの節で取り上げるほどには十分開発されていない．

5.2 共振器量子電気力学実験: 共振器の原子とイオントラップ

(*H. C. Nagerl, D.Leibfried, F.Schmidt - Kaler, J.Eschner, R.Blatt, M.Brune, J.M.Raimond, S.Haroche*)

5.2.1 量子振動子と結合した 2 準位系

光共振器中の原子，あるいはトラップ中のイオンは，よい近似として，量子調和振動子に結合した 2 準位系であると考えることができる．光共振器中の原子の場合には，1 個の 2 準位原子が共振器の共鳴モードに結合する．トラップ中のイオンの場合には，一つのイオンがもつ二つの内部状態（超微細構造準位 あるいは準安定のエネルギー準位）が，トラップ中のイオンの振動の自由度に結合する．このように，両方のシステムは同じ相互作用によって特徴づけることができる．相互作用（ジェインズ–カミングス）ハミルトニアン [159] は

$$H_{\rm int} = -\hbar \frac{\Omega}{2}(a\sigma^{+} + a^{\dagger}\sigma^{-}) \tag{5.1}$$

と書くことができる．ここで，a と $a^{\dagger}$ は量子振動子の消滅と生成の演算子，また，σ^{+} と σ^{-} は 2 準位系の上昇下降演算子， Ω は結合振幅である．このハミルトニアンは，原子もしくはイオンの遷移と関連した，光子（共振器量子電気力学実験の場合）あるいはフォノン（音子）（イオントラップの実験の場合）の放出あるいは吸収を記述する．調和振動子モードが 2 準位系に対してちょうど共鳴条件にあるとき，相互作用の項は実際のエネルギー交換を記述する．系が共鳴状態にないときには，エネルギーの移動は仮想的なものになる．そして，その相互作用は原子準位の位相シフトをもたらす．

鍵になるのは，どのように強結合状態を実現するかである．その状態では原子の自然放出，光子/格子振動緩和，および熱雑音によって起こされるデコヒーレンスなどのすべての緩和過程を，式 (5.1) の単純な相互作用が圧倒することになる．最も単純な物質–場の系を，実験的に十分に実現することによって，基礎的な量子論理演算を実行することが可能になる．同時に，それは量子理論の最も直観的に理解しにくい面についてのわれわれの理解に対する厳しいテストを提供する．たとえば，非局所的なエンタングルメントや， メゾスコピックな重ね合わせ状態などである．

共振器量子電気力学は，光学的な領域とマイクロ波の領域の両方において発展した．それらの実験の基本的な原理はきわめて似ている．これらの二つの分野の実験のレビューについては[160]を見よ．光学的な領域では，光学的な原子遷移は，非常に高いフィネスをもつ共振器に結合される．そのような強結合状態は実現され，研究されてきた．この節ではマイクロ波領域に焦点を合わせる．長寿命でかつ容易に検出可能な円形のリュードベリ(Rydberg)原子は，高いQ値の超伝導体の共振器中に閉じこめられたミリ波の放射に強く結合する．熱運動速度で移動する原子は，共振器を横切る際に，場のモードともつれ合う．共振器中の場の寿命と，原子の2準位系の寿命の両方は，相互作用時間よりずっと長い．そのために，原子が共振器を去った後でも，共振器中の場と原子はエンタングルしたままでいる．このように，共振器の場と原子とからなる量子状態を，思うままにさらに研究したり，また操作することが可能である．

この章で触れる二つめの種類の実験は，調和振動子型の電磁トラップに束縛されたイオンに関するものである．量子振動子はこの場合，イオンの特定の振動モードである．それは，レーザパルスを介して，2準位系として記述できるイオンの内部準位に結合する．適切なレーザ光パルスの存在下では，イオンの振動と内部準位の間の相互作用は，非常によい近似で，ジェインズ–カミングス型のハミルトニアンによって記述することができる．イオンを用いた周波数標準のために開発された技術によって，2準位系と振動モード双方の長いコヒーレンス時間を達成することができる．

完全に異なった実験的な環境にもかかわらず，原子–共振器系とイオントラップの実験によって同じ単純なモデルを実現することができる．そのために，共振器量子電気力学のために立案されたどんな実験でも，イオントラップという状況に翻訳することができ，そして逆もまた同様である．さらに，これらの二つの技術によって成し遂げられた成果は非常に似ている．次の節では，マイクロ波領域の共振器量子電気力学実験，およびジェインズ–カミングス相互作用を含むイオントラップ実験について見ていく．その後，それら両方の技術を用いた量子計算の展望について述べる．

5.2.2 原子と共振器による共振器量子電気力学

マイクロ波共振器中の原子を用いた共振器量子電気力学実験の一般的な仕組みについて説明する．実験上，理論上の詳細については，他の文献を参照せよ [160,161].

円形リュードベリ原子は，共振器量子電気力学実験の実現のために前例のない手段を提供する．これらの原子は，非常に高いエネルギーをもつ．その主量子数 n は 50 前後で，また最大の方位量子数と磁気量子数を有し，ミリ波輻射に強く結合した巨大なアンテナのように振る舞う．51.099 GHz の円形状態 $n = 51(|e\rangle)$ と $n = 50(|g\rangle)$ 間の遷移についての双極子行列要素は，1250 原子単位程度の大きさをもつ．水素原子型多重度にある他の準位との混合をさけるために，原子を弱電場中に置いた場合，これらの準位は 30 ms のオーダの長い寿命をもち，本当の 2 準位系として振る舞う．さらに，電界イオン化法によって，状態を選択しながらかつ高い感度でこれらの原子を検出することが可能である．

ミリ波領域では，超伝導体を用いることで，非常に高品質の共振器を構成することができる．ニオブ製の鏡を用いた，センチメートルサイズのファブリペロ型共振器が実験で使われる．0.6K のような低い温度においては，Q 値は 10^8 から 10^9 に達する．これは，光子蓄積時間 T_r に換算すると，数百マイクロ秒から数ミリ秒までに相当する．それは熱運動速度の原子について，数十マイクロ秒である原子–共振器相互作用時間よりずっと長い．これらの低い温度において，熱の影響は十分無視することが可能であり，共振器を基底状態で見いだす確率は 98% 以上である．

パリの Ecole Normale において用いられた実験装置 [164]-[168] を図 5.1 に示す．その主要部分は ^{3}He-^{4}He 冷却器によって 0.6K に冷却される．原子は最初，炉 O から流れ出，V の領域で速度選択がなされる．その速度選択は，原子線の伝播する方向に対してある一定の角度で入射するレーザ光線を用いた，速度選択的な光ポンピングにより行われる．速度選択された原子は箱 B において，一連のレーザパルスとそれらに伴う断熱的なラジオ波の遷移によって，状態 $|e\rangle$ あるいは $|g\rangle$ の一つに，箱 B において準備される．この状態準備はパルス状になされ，明確な時刻に 200～400m/s の間で ±2m/s の正確さで速度が制御された円形原子のバースト（小爆発的な射出）が得られる．原子の

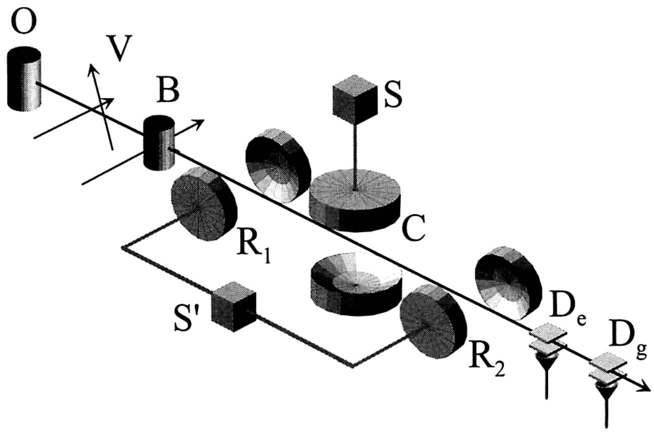


図 5.1　原子－共振器実験装置

位置は ±1mm の精度でいつでも確定できる．そのため，装置を通過する異なる原子のそれぞれに対して，選択的に（ユニタリ）変換を施すことができる．それぞれのバースト内の平均原子数は 1 以下に保たれるため，同時に二つの原子が準備される確率は小さい値に押さえられる．

超伝導の共振器 C は二つの球形のニオブ鏡から作られていて，それらは 2.7 センチ離れている．それはビームウエスト 6 ミリのガウス型横モードの電磁場を形成する．必要に応じて，共振器のモードは次の 2 通りの方法で励起される．一つは，原子と場との共鳴的な結合を通じて，あるいは，マイクロ波源 S からのコヒーレントな振動場の入射によってである．共振器のミラー間距離を調整したり，あるいはミラーを横切って印可される電場によって原子の遷移周波数を変化させることで，共振器を原子の遷移周波数と同調させたり同調させなかったりすることが可能である．

C に入射する前に，原子は低い Q 値の補助共振器 R_1 を横切る．そこで，古典的なマイクロ波パルスによって準位 $|e\rangle$ と $|g\rangle$ を混ぜることができる．それぞれの原子は，C を数十マイクロ秒かけて横切り，その間，原子と共振器の場とは強く相互作用する．共振器の中心にある原子に対して，原子と場との結合振幅（ジェインズ–カミングス相互作用の Ω）は $\Omega/2\pi = 50$ kHz である．これは原子と共振器モード間の単一光子の交換レートに対応する．原子が共振器を横切って動くとき，結合定数 $\Omega(\mathbf{r})$ はその位置に関するガウス関

数で与えられる．C の後で，補助共振器 R_2 において，古典的な共鳴マイクロ波のパルスにより $|e\rangle$ と $|g\rangle$ が再び混ぜられる場合もある．最終的に，原子は二つの電界イオン化検出器 D_e と D_g に達する．それらは状態分離が可能で，それぞれ 40%の効率で状態 $|e\rangle$ と $|g\rangle$ にある原子を計数可能である．

1 回の実験手順は次のようなものである．一つ，あるいは十分な間隔をあけた二つの原子を実験系に送り込み，それらを検出器 D_e または D_g によって検出する．同じ実験手順が，1.5 ms の繰り返し周期で多数回繰り返される．1.5 ms は共振器の減衰時間よりも長いため，共振器 C の中の場はそれぞれの実験の開始時点でいつも同じ初期状態にある．これらの実験を繰り返し行った結果は統計的に解析される．2 原子相関の確率を求めるためのサンプル数は，約 2 時間の実験で記録されるうち，典型的には 15000 件である．二つのタイプの実験が行われた．5.2.3 項で示される第 1 の実験では，原子と共振器モードは完全に共鳴している．そのため，エネルギー交換を通じて，原子と場のエネルギーのもつれ合いが生じる．5.2.4 項で示される第 2 の実験では，原子と共振器は共鳴条件にない．そのため，相互作用は原子もしくは共振器のエネルギーシフトを引き起こし，その結果位相もつれ合いが生じる．

5.2.3 共鳴結合：ラビ振動と，エンタングルした原子

ここでは，共振器が原子の $|e\rangle \to |g\rangle$ 遷移と共鳴するように調整されている場合を考える．連続的な原子の流れの元，単一光子は共振器 C 中の単一原子により放出，あるいは吸収されることが可能である [161]-[169]．この累積的な放出は，マイクロメーザの動作へとつながる [170]．このような単一光子－単一原子相互作用系は，量子ラビ振動 [171]，場の量子化の直接的な証拠，量子メモリ [167]，二つの原子の間の量子エンタングルメント [168]，および単一光子の吸収を伴わない検出 [169] などの実演に用いられてきた．

最も単純な実験は，準位 $|e\rangle$ の原子一つを送り込み，それが $|e\rangle$ から $|g\rangle$ へとフリップする確率を測定することによって行われる（領域 R_1 と R_2 は用いられない）[165]．そのとき，原子の速度を変えたり，あるいは横断時間の間だけ原子の遷移（周波数）を共振器にシュタルク効果を用いて調整することにより，原子－共振器相互作用時間 t を種々変えながら測定は繰り返される．

共振器場がはじめ真空状態にある場合について，実効的な相互作用時間 t に対するラビ振動信号を図 5.2(A) に示す．図中，点は実験値を示し，また曲

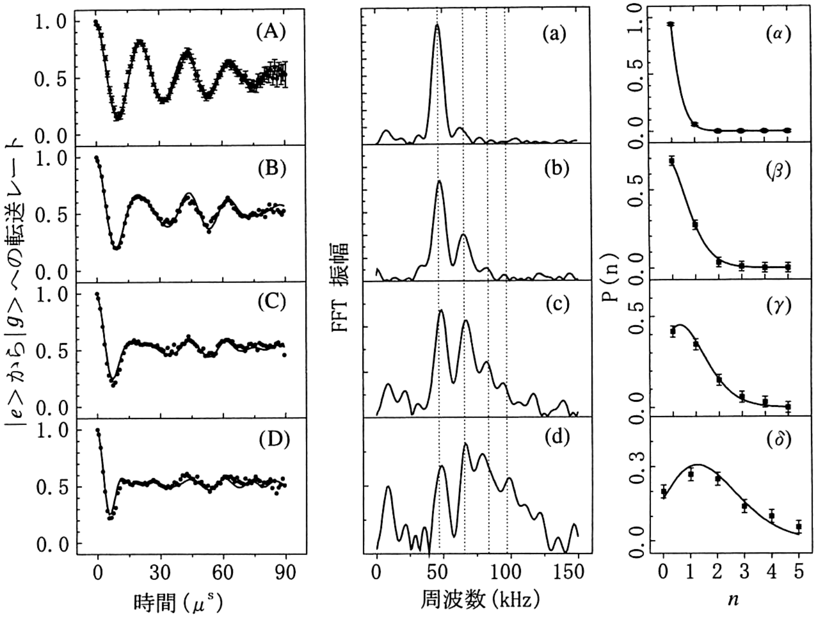


図 5.2　量子ラビ振動．(A), (B), (C) および (D)：ラビ歳差信号 (A)：入射場なし，平均熱光子数 0.06 (±0.01)；(B), (C), および (D)：平均光子数 0.40 (±0.02), 0.85 (±0.04) および 1.77 (±0.15) のコヒーレント場．点は実験値; 実線は理論フィット．(a),(b),(c),(d)：対応するフーリエ変換．一連の整数値の平方根に対応する周波数を，垂直線で示す．(α), (β), (γ), (δ)：実験の信号（点）から推測した光子数分布．実線：熱分布 (α) または コヒーレント分布 ((β), (γ), (δ))

線が理論的なフィッティングを示す．実効的な相互作用時間 t を実験的なパラメータから計算する際には，共振器の中でのカップリングのガウス分布的な変化を考慮に入れている．$\Omega/2\pi$ =50 kHz に振動数が近いとき，四つの完全なラビ振動が観測される．それらは基本的な ジェインズ–カミングス過程，つまり「1 光子の放出と吸収に対応した，$|e\rangle$ と $|g\rangle$ 間の原子の反転可能な時間発展」に相当する．振動の減衰は，実験的な不完全性によって生じている．この真空ラビ振動の信号は，原子と空の共振器からなる系のスペクトルに見られる真空ラビ分裂の時間領域における対応物である．

図 5.2(B～D) に，平均光子数がそれぞれ $n = 0.40(\pm 0.02)$，$0.85(\pm 0.04)$，そ

して 1.77(±0.15) のコヒーレント場が共振器に最初存在する場合の振動のシグナルを示す．この振動は，共振器場に存在している種々の光子数に対応して，いくつかの周波数成分を含んでいる．それらの間のビートによって，振動の消失と再現が生じる [171]．図 5.2 (a～d) に示されているラビ信号のフーリエ変換は，場に光子が n 個 (n =0～3) 含まれるときのラビ振動数 $\Omega\sqrt{n+1}$ のところにピークを示している．つまり，古典場に対しては比例するはずのラビ振動数は，実際には不連続量だということである．この事実は，**箱の中での場の量子化の直接の証拠**になっている．図 5.2(α～δ) にフーリエ成分の振幅を示す．それぞれの振幅は，直接，光子数分布を示している．図 5.2(a) で，$\Omega\sqrt{2}$ に見られる小さなピークは，残留した熱の場によるものである．それは，0.8K において 0.06 の平均光子数に相当する．

場のエネルギーの量子化の直感的な証拠を提供することに加えて，この実験は原子–共振器の共鳴的な相互作用が緩和プロセスに優越していることを示している．また得られる原子–場のもつれ合いは，量子エンタングルメントを生成または操作するのに利用できるため，基礎的な量子計算の操作への基礎も提供している．

原子–場のもつれ合いは，最初に非常に単純なデバイス，空洞内に一つの単一量子ビットを保持する量子メモリ，を実現するために用いられた．このメモリは，最初の原子によって書き込まれ，そして次の原子によって読み出される．最も単純な場合，最初の原子は状態 $|e\rangle$ で，空の共振器に入る．実効的な相互作用時間 t は $\Omega t=\pi$ を満たすとする．そのとき，原子は C から状態 $|g\rangle$ で出て，C に 1 光子状態を置き去りにする．2 番めの原子は，ある遅延時間 T の後で状態 $|g\rangle$ で共振器に入射する．そして，自然な緩和が生じていなければ，この光子を吸収して，最終的に状態 $|e\rangle$ になる．2 番めの原子を見いだす $|g\rangle$ での確率 T に対する減衰は，共振器中での単一光子の寿命を与える．当然ながら，それは古典場のエネルギーの減衰時間 T_r に等しくなる [167]．

また R_1 内で，マイクロ波の $\pi/2$ パルス（周波数 ν）を照射して，$|e\rangle$ と $|g\rangle$ の等分の重ね合わせ状態にあるように準備した原子を，空の共振器内に送り込むことも可能である．原子状態のうち $|e\rangle$ 成分は，確率 1 で光子を C で放出するが，一方 $|g\rangle$ 成分は変わらずにいる．それゆえ，原子の重ね合わせ状態は，場が 0 個の光子と 1 個の光子の重ね合わせ状態になるように転写され

る．そして，原子は C を出るときには，状態 $|g\rangle$ になる．C での場は，平均光子数が 1/2 と等しく，かつ，R_1 のマイクロ波と直接関係をもつような明確な位相をもっている．位相情報はその原子によって，R_1 から C に運ばれたことになる．

場は，遅延時間 T の後に，状態 $|g\rangle$ で準備された 2 番めの原子によって読み出される．そのとき，2 番めの原子は C において π パルスを経験することになる．量子コヒーレンスはこのとき，$|e\rangle$ 状態と $|g\rangle$ 状態の重ね合わせとしてこの原子の上に転写される．そして，共振器 C は空になる．R_2 では，$\pi/2$ パルスが照射される．このパルスは，最初の原子が R_1 において受けたものと同じ振動数 ν と位相をもつ．空洞 R_2 とそれに引き続く D_e, D_g は，第 2 の原子に対する，位相情報をも含めた重ね合わせ状態の検出器として働く．$|e\rangle$ あるいは $|g\rangle$ でこの原子を発見する確率は，通常のラムゼイ干渉縞と同様に ν に対して振動する．しかし通常の場合と異なり，二つのパルスは二つの異なる原子に作用し，コヒーレンスはそれら原子間で空洞場 C を介して移される．図 5.3(a)～(c) に見られる干渉縞は，原子間で三つの異なる時間間隔を置いた場合についてのコヒーレンス移動を示している．時間が増すと，干渉縞の周期と振幅は減少する．このコントラストの低減は，C における場の減衰を明らかにする．この実験は $|1\rangle$ と $|0\rangle$ のフォック状態（光子数状態）を含んでおり，また後者は減衰しないため，減衰時間は T_r に比べて 2 倍である．

この実験で，量子ビットが 二つの原子の間で一つの 1 光子場を介して受け渡される．中間状態で，空洞場は，1 光子状態と 0 光子状態の非常に非古典的な重ね合わせ状態にある．このような原子から場への転写過程は，提案されている共振器量子電気力学量子ゲート [174] の実現に不可欠である．

同じ方式が，少し異なった条件の下で，非局所的な原子と場の間，あるいは原子−原子間のもつれ合いを準備したり操作するのに用いられるかもしれない [175]．第 1 の原子は，状態 $|e\rangle$ で空の空洞に送られ，そこで $\pi/2$ パルス ($\Omega t = \pi/2$) を施される．そして，原子と共振器は $|e,0\rangle + |g,1\rangle$ というエンタングルメント状態になる．そのとき，状態 $|g\rangle$ で準備された第 2 の原子を，$\Omega t = \pi$ となるような相互作用時間で C を通過するように送り込むことによって，原子−原子間のエンタングルメントを生成できる．第 1 の原子によって残された光子は確率 1 で第 2 の原子によって吸収され，空洞は空になり，原

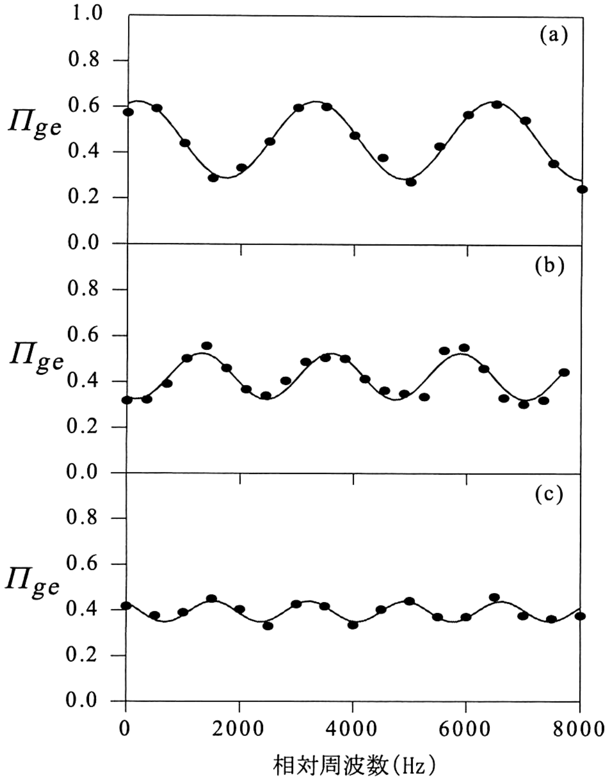


図 5.3 2 原子間でのコヒーレンスの移動: 最初の原子が $|g\rangle$ で検出される場合に，第 2 の原子を $|e\rangle$ で検出する条件付確率 $\Pi_{ge}(\nu)$ を，最初の原子に対しては R_1 で，第 2 の原子に対しては R_2 で照射するマイクロ波パルスの周波数 ν に対してプロットした．R_1 と R_2 での二つのマイクロ波パルス間の遅延時間は，(a) から (c) に対してそれぞれ 301, 436, および 581 μs である

子は次のエンタングル状態になる．

$$|\Psi_{\mathrm{EPR}}\rangle = \frac{1}{\sqrt{2}}\left(|e_1, g_2\rangle - |g_1, e_2\rangle\right) \tag{5.2}$$

ここで，添え字は第 1 と第 2 の原子を指す．

これは，もつれ合った粒子の Einstein-Podolsky-Rosen (EPR) 対である [21]. 原子は，スピン 1/2 の粒子として記述できる．$|e\rangle$ と $|g\rangle$ の状態はそれぞれ，ある方向 Oz に量子化された +1/2 と −1/2 の状態に対応する．そのとき，$|\Psi_{\mathrm{EPR}}\rangle$ は回転に対して不変な「スピンゼロ」の状態となる．つまり，任意の量子化軸に対して常に互いに逆向きの状態で検出されるという意味において，これらのスピンは反相関関係にある．これを例証するために，xOy 平面内に Ox 軸と ϕ の角度をなすある軸をとる．この軸に沿ったスピンの固有ベクトルは形式 $|e\rangle \pm e^{i\phi}|g\rangle$ という状態をとる．そして状態 $|\Psi_{\mathrm{EPR}}\rangle$ は，（全体にある位相因子がかかっているとして）次のように書ける．

$$|\Psi_{\mathrm{EPR}}\rangle = (|e_1\rangle + e^{i\phi}|g_1\rangle)(|e_2\rangle - e^{i\phi}|g_2\rangle) - (|e_1\rangle - e^{i\phi}|g_1\rangle)(|e_2\rangle + e^{i\phi}|g_2\rangle) \tag{5.3}$$

これは，反相関関係を示している．

エネルギー基底（Oz 軸）におけるエンタングルメントを解析するために，原子が C から出た後の状態を検出する．理想的には，$|e\rangle$ と $|g\rangle$ の種々の組み合わせで原子を検出する確率は，$P_{eg} = P_{ge} = 1/2$, $P_{ee} = P_{gg} = 0$ になるはずである．われわれはそのかわりに，$P\mathrm{eg} = 0.44$, $P\mathrm{ge} = 0.27$, $P\mathrm{ee} = 0.06$, $P\mathrm{gg} = 0.23$ を得た．その差は，二つの原子の通過の間に C に蓄積された光子の減衰や，他のさまざまな不完全性のためである．定量的な解析により，原子の EPR 対が 63%の純度 (purity)[168] で作り出されたことがわかった．

式 (5.3) によって表現される反相関の性質は，R_2 において両方の原子に $\pi/2$ パルスを適用することによって解析される．R_2 でのスピン回転とそれに引き続く Oz 方向での検出により，水平面内のある量子化軸についての状態検出を行うことができる．より具体的には，R_2 の後で $|e\rangle$, $|g\rangle$ どちらの状態で検出されるかは，R_2 の前で原子が重ね合わせ状態 $|e\rangle \pm e^{i\phi}|g\rangle$ のどちらの状態に存在したかに対応する（+符号のとき $|e\rangle$）．ここで，ϕ は R_2 において加えられるパルスの位相である．反相関関係から，この測定により第 2 の原子は，第 1 の原子の測定された方向と逆の方向を指す重ね合わせ状態に射影される

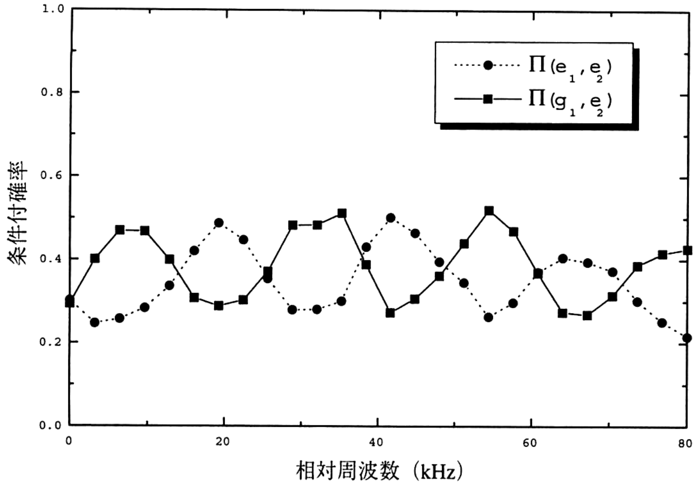


図 5.4 原子の EPR エンタングルメント：最初の原子が $|e\rangle$ で検出される場合に，原子を $|e\rangle$ で検出する条件付確率 $\Pi(e_1, e_2)$ （黒丸），および最初の原子が $|g\rangle$ のときの確率 $\Pi(g_1, e_2)$（四角）を，R_2 でのパルスの周波数 ν に対してプロットした．実験点の間をつないでいる線は，見やすくするために付加した

はずである．両方の原子が同時に R_2 を通過する場合，$|e\rangle$ と $|g\rangle$ 探知器の間で完全な反相関関係が観察されるだろう．実際には，2 番めの原子は T だけ遅れるため，第 2 の原子と R_2 における場の間のコヒーレンスは，時間間隔 T の間歳差運動をする．$|e\rangle$ あるいは $|g\rangle$ で 2 番めの原子を発見する最終的な確率は，原子のコヒーレンスと R_2 におけるマイクロ波の間で蓄積された位相による．この位相のシフトは，原子とラムゼイ場の周波数差，および飛行時間 T に比例する．これは再び一種のラムゼイ干渉縞の状態である．しかしながら，二つのマイクロ波パルスは異なった原子に照射され，そして位相は非局所的な量子相互関係を通してそれら原子間で受け渡される．

図 5.4 に，ラムゼイ帯の周波数 ν に対する条件付き確率 Π_{e_1,e_2} および Π_{g_1,e_2} を示す．Π_{e_1,e_2} (Π_{g_1,e_2}) は，最初の原子が $|e\rangle$ ($|g\rangle$) で検出されたときに第 2 の原子が $|e\rangle$ で検出される確率である．このグラフの上がり下がりから，2 番めの原子の状態のコヒーレンスが明らかになる．これら二つの確率は位相が逆になっている．これは，第 1 の原子が $|e\rangle$ ではなく $|g\rangle$ で検出されると，第 2

の原子の位相が π 変化するからである．

この実験データは，二つの量子ビットの制御されたエンタングルメントを準備できることを実証している（ここで，二つの原子は 1.5cm 離れている）．共鳴的な相互作用と分散的な相互作用を組み合わせることで，この方式は原子が $|e,e,e\rangle - |g,g,g\rangle$ の式で表される「三つ子」状態の準備へと拡張することができる [175]-[177].

原子と場の共鳴的な相互作用は，共振器内に蓄えられた光子を吸収せずに検出することにも用いられてきた [169]．原子が共振器を準位 $|g\rangle$ で通過するとき，単一光子場において 2π のラビ振動を受けて起こる条件付き位相シフトがこの方法の重要な点である．原子が空の共振器（初期状態 $|g,0\rangle$）を通過する際には，相互作用に影響されない．共振器が 1 光子を含むとき，原子–共振器系は $|g,1\rangle \to -|g,1\rangle$ の変換を受ける．全体的な波動関数の π 位相シフトは，実空間において一つのスピン 1/2 の 2π 回転と同様である．この条件付き位相シフトは，準位 g から，共振器場と結合していない参照準位 i への遷移に関するラムゼイ干渉によってテストすることができる．位相シフトの観察は共振器において光子を検出することに等しい．たいていの光検出器とは異なり，光子は「測定器」原子との相互作用の後に共振器に残される．だから，この実験は単一光子場の量子非破壊測定に等しい．ただしその単一光子場は，0 光子と 1 光子状態によって構成される部分空間に限定されている．さらに，この方法の核心である条件的なダイナミクスは，一つの量子論理ゲートとして見ることもできる．

5.2.4　分散的な結合：シュレーディンガーの猫とデコヒーレンス

原子の遷移周波数 ω_0 と，場のモード周波数 ω が δ だけ異なる場合を考えよう．ここで，δ は Ω および共振器の線幅よりも大きいものとする．この状況では，エネルギー保存が原子による光子の放出や吸収を妨げ，そして共振器との相互作用は純粋に分散的になる．前節で述べたように，原子と場のエネルギーエンタングルメントは,「原子の状態」と「放射電磁場の位相」のエンタングルメントに置き換えられる．ここで，放射電磁場は古典的なものと見なしてよい．つまり，微視的な自由度が,「巨視的」な量をコントロールする．このエンタングルメントは量子測定の原形であり，これによりわれわれは通常とは異なるスケールで，量子力学の不可思議さを調べることが許される．

C において，円形のリュードベリ原子を小さなコヒーレント場と相互作用させる．ここで，場の振幅 α および平均光子数 $|\alpha|^2$ は，典型的には 0 から 10 の間とする．真空ラビ振動数は，原子の共振器中での位置についてガウス関数であるので，相互作用は断熱的にオン，オフされる．このため，原子–共振器離調（デチューニング）が小さい場合 ($\delta/2\pi = 100$〜700 kHz) でさえ，原子と共振器場の間の光子の交換はほとんど起こらない．そのために，相互作用は周波数シフト（ずれ）だけをもたらす．原子が共振器の中心に存在するとき，共振器モードは $\pm\Omega^2/4\delta$ だけずれる．単一原子の屈折率の効果により，原子が $|e\rangle$ または $|g\rangle$ の状態にあるかで，このずれはそれぞれ逆の値をとる [161]．それは，$\delta/2\pi = 100$ kHz の場合で ±6 kHz に達する．この値は，「普通の原子」一つあたりの屈折率に対して 15 桁ほど大きな値である．

単一原子の共振器内の通過によって引き起こされる周波数シフトは，コヒーレントな共振器場を，$\pm\Phi = \pm\Omega^2 t/4\delta$ だけ位相シフトする．ここで t は実効的な相互作用時間である．位相シフトは典型的に 1 ラジアンのオーダである．この原子–場相互作用は，それぞれ異なった位相をもった場の状態の非古典的な重ね合わせを生成するために用いることができる．原子は R_1 で $\pi/2$ パルスによって，$|e\rangle$ と $|g\rangle$ の重ね合わせ状態に準備される．原子が C を横切るとき，それは同時に場に二つの反対の位相ずれ $\pm\Phi$ を与える．結合された原子と場の全系は，次の状態になる．

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|e, \alpha e^{i\Phi}\rangle + |g, \alpha e^{-i\Phi}\rangle\right) \tag{5.4}$$

この状態は，原子のエネルギーが場の位相と相関しているような，エンタングルした状態である．コヒーレント状態は図 5.5(a) に示すように，位相空間において一つの矢印で示すことができる．そのとき，矢印の長さと方向は，それぞれ振幅と位相に対応している．矢印の先端の単位円は，場の量子的な不確定性を表している．式 (5.4) によると，この矢印は「測定針」と見なすことができる．図 5.5(b) に示すように，その針のそれぞれ異なる方向が，原子の状態に対応すると見ることができる．この相互作用によって,「測定」を行うことが可能になる．測定においては,「場の矢印」が原子のエネルギーを決定するために用いられる．あるいは，シュレーディンガーの隠喩を採用してもよいだろう [178]．つまり，場の $+\Phi$ と $-\Phi$ の成分は，有名なシュレーディンガーの猫の「生きている」状態と「死んでいる状態」に対応していて，それ

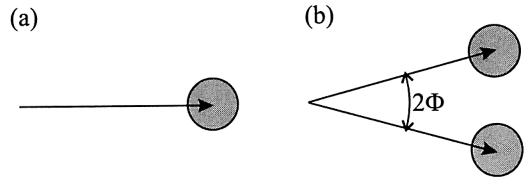


図 5.5　(a) コヒーレント場状態の位相空間上での図示．(b) 原子状態 $|e\rangle$ と $|g\rangle$ と相関をもつ場 (5.4) の成分

らは原子の励起状態と基底状態とエンタングルしている，という風に．

共振器を通過した後，検出される前に，原子は R_2 においてもう一度 $\pi/2$ パルスを受ける．その位相は R_1 でのパルスとコヒーレントである．原子を $|g\rangle$ 状態で検出する確率 P_g が，R_1 および R_2 で加えられる電磁波の周波数 ν の関数として測定される．図 5.6(a) は，離調 $\delta/2\pi = 712$ kHz で，共振器内に光子が存在しない場合の実験結果である．原子の状態が $|e\rangle$ から $|g\rangle$ に遷移するのは，R_1 における場合（c を状態 $|g\rangle$ で通過）と R_2 における場合（c を状態 $|e\rangle$ で通過）の 2 通りある．原子が共振器の中にその痕跡をまったく残さないので，これらの二つの経路は区別できない．そのため，それらに対応する振幅は干渉し，P_g の振動（ラムゼイ干渉縞）として現れる．

図 5.6 (b〜d) は，コヒーレントな共振器場が平均 9.5 の光子を含んだ場合について，原子−共振器の離調を減少させていった実験結果である．離調がより小さいと，それだけ C における場の成分の分離は大きいだろう．図 5.6 (b〜d) の挿入図は，原子状態の記録である場の位相情報を図示したものである．相補性原理によると，このような Welcher - Weg（which-way, どちら側）情報は，たとえ読み出されなくても，干渉効果を破壊するに違いない．定量的な解析によれば，この干渉縞信号は二つの場の成分の重なり積分によって定まり，その積分の大きさは縞のコントラストに，位相はラムゼイ干渉縞の一つに影響を与える．Φ が大きいと重なりは小さく，干渉縞は姿を消す．Φ が小さければ，干渉縞は減少したコントラストではあるが観察される．検出信号から，共振器が原子状態の計測器として働くことが十分に示されている．さらに，より大きな離調に対しての縞の位相シフトから，光子数を正確に決定することができる．

共振器を通過する原子に対する以上のような準備と検出の方式によって生

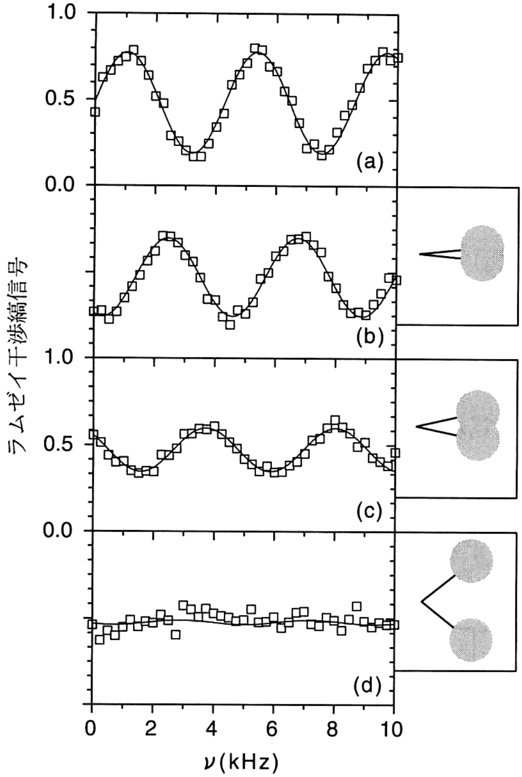


図 **5.6** 原子を $|g\rangle$ に見いだす確率の，ν に対するプロットに見られるラムゼイ干渉縞: (a) C 空，$\delta/2\pi = 712$ kHz; (b) から (d) $|\alpha| = \sqrt{9.5} = 3.1$ で，それぞれ $\delta/2\pi = 712$，347 および 104 kHz のコヒーレント場が C に存在する場合．点は実験値で，曲線は正弦波フィット．挿入図は，C に残された場の成分の位相空間表示

じる，メゾスコピックな場の量子重ね合わせはもろく，特に $|\alpha|^2$ や Φ が大きいときにはデコヒーレンスを受ける [179-186]．量子重ね合わせ状態から統計的な混合状態への時間発展をモニターするために，場の「猫状態」は，共振器を時間 T 遅れて通過する第 2 の原子によって探られる [166,186].（第 2 の）探査原子は最初の原子と同じ位相ずれを引き起こす．それは最初の原子によって起こされた二つの場の成分のそれぞれを，さらに二つの部分に分ける．これは，場の最終状態は，それらの二つがゼロ位相で一致するような，四つの

状態になることを意味する．二つの原子が，$|e\rangle,|g\rangle$ または $|g\rangle,|e\rangle$ の組み合わせで通過するとき，位相は初期値へと戻る．R_2 において原子状態が混ぜあわされた後では，$(|e\rangle,|g\rangle$ または $|g\rangle,|e\rangle$ の）いずれの経路（組み合わせ）をたどったのかの情報はもはやない．これは，第 1 の原子によって場に残された情報が，第 2 の原子によって部分的に消去されたからである [187]．これらの二つの経路の寄与は，結合確率 P_{ee}, P_{eg}, P_{ge} および P_{gg}，ならびに相関信号 $\eta = P_{ee}/(P_{ee}+P_{eg}) - P_{ge}/(P_{ge}+P_{gg})$ に干渉項の存在となって現れる．

もし重ね合わせ状態が T の間生き残っていれば，η が理想的に値 1/2 をとるのに対して，場の状態が単なる統計的な混合状態であるときそれは消失する．二つの異なる「猫状態」（挿入図を参照）について，η を T に対して測定した結果を図 5.7 に示した．点は実験値で，実線および点線は理論値である [188]．最大値が 0.18 にとどまるのは，ラムゼイ干渉計のコントラストが限定されているためである．猫成分の間隔が広がると，デコヒーレンスが共振器の減衰時間よりずっと短い時間に生じ，より効果的である．そのとき定数

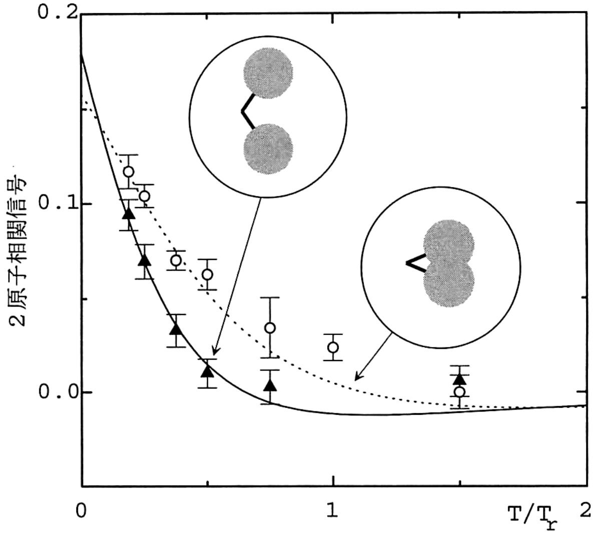


図 5.7　シュレーディンガーの猫のデコヒーレンス: $\delta/2\pi = 170$ kHz（白丸）および $\delta/2\pi = 70$ kHz（三角）での，T/T_r に対する 2 原子相関信号 η．破線と実線は理論値．挿入図: 2Φ 隔たった，対応する場の成分の図示

が初期状態に強烈に依存するような，非自明な緩和メカニズムが観察できる．デコヒーレンスは共振器から外部への光子の損失が原因である．それぞれの「逃げ出す」光子は，C の中に蓄えられていた位相の情報を環境中にコピーする小さな「シュレーディンガーの猫」として記述することができる．この「漏れた」情報が読めたかもしれないという事実だけで,「猫」の量子コヒーレンスに関連した干渉効果を消し去るのには十分である．この点から，デコヒーレンスは相補的な現象である．上に示されたシュレーディンガーの猫状態の短いデコヒーレンス時間（約 $T_{\rm cav}/n$）は，このような考え方によって説明される．光子数がより大きいと，環境の中に一つの「光子コピー」を漏らすために必要な時間はより短くなる．この実験はデコヒーレンスの基本的な特徴を確認し，そして大きい系での量子コヒーレンスの壊れやすさを鮮やかに示している．量子力学的な重ね合わせ状態がマクロな規模へ拡大すると，ほとんど直ちにデコヒーレンスが生じる．これは，どんな実際的な目的に対しても量子測定のコペンハーゲン解釈が有効であることを示している．この実験は，大きな規模での量子エンタングルメントを生成し制御するために克服されなければならない困難について，興味深い洞察を与える．すなわち，量子デコヒーレンスは大規模な量子情報処理に対する主要な制限として現れる．量子誤り訂正法を用いない場合の，量子計算の限界についてのさらなる議論は，7.3 節において与えられる．

5.2.5　イオントラップ実験

ラジオ周波数の Paul トラップ内の一つまたは小数個のイオンは，単純な量子系のダイナミクスを調べるのに理想的な環境である．そして，レーザパルスを用いることで，研究者はその単純な系の相互作用をほとんど意のままに仕立て上げることができる．特に興味深い筋書きは，前章で記述された共振器量子電気力学の光子場を，外部の束縛ポテンシャル中のイオンの振動を記述する調和振動子によって置き換えるというものである．次の形式の相互作用ハミルトニアンのように，適当な光の場は，イオンの二つの内部電子準位 $|g\rangle$,$|e\rangle$ を，周波数 ω の外部の振動と結合することができる [189]-[192].

$$H_{\rm int} = -\hbar G\left(\sigma^{+}e^{i\eta(a^{\dagger}+a)-i\delta t} + \sigma^{-}e^{-i\eta(a^{\dagger}+a)+i\delta t}\right) \tag{5.5}$$

ここで，$\eta = \delta k\sqrt{\hbar/(2m\omega)}$ はラム－ディッケ・パラメータ，この係数 δk は波数（あるいは，ラマン遷移によって結合される場合は波数ベクトルの差），$(a^\dagger + a)$ は調和振動子の昇降演算子を用いて書かれた位置の演算子，そして G はカップリング光の振幅に比例する結合強度である．この相互作用ハミルトニアンはジェインズ－カミングス・ハミルトニアン (5.1) より本質的により複雑である．しかし，二つの内部状態のエネルギー差に対して光を $\delta = -\omega$ だけ離調した場合で，かつ $\eta\sqrt{\langle(a^\dagger + a)^2\rangle} \ll 1$ の極限においては，ジェインズ－カミングス・ハミルトニアンへと簡約される．一般に，$\delta = (n' - n)\omega$（n, n' は整数）の任意の離調は，$|g, n\rangle$ と $|e, n'\rangle$ 状態の間の遷移を共鳴的に駆動し，その結果別の実効的な相互作用ハミルトニアンになる．さらに，前の章で議論した場合とは異なり，結合強度 G は双極子行列要素と共振器のモード体積によって固定されるのではなく，光の強度を適切に選択することで変化させうる．

研究室内で上に記述した状況を実現するための技術は，捕縛された冷却原子を用いての周波数標準を作りあげる努力の中から生み出された．荷電粒子のラジオ周波数 (rf) トラップ内への動的なトラップは，はじめ W.Paul によって 1958 年に提案され，また彼の手で実験的に検証された [196]．適当な電極の構造によって生み出される rf 電場が，帯電粒子を閉じ込めるための疑似ポテンシャルを形成する [197]．単一のイオンをトラップするための電極は，だいたい数ミリメートルから小さくて 100μm 程度の大きさをもつ．rf 場は，10～300MHz の範囲で，ピーク・ツー・ピークで数百ボルトである．このような場の中に閉じ込められた粒子の運動は，加えられている駆動周波数と同期した早い成分（微小運動）と，動的に作り出された疑似ポテンシャル中の遅い（永年）運動の成分をもつ．四重極 (rf) 場構造に対しては，疑似ポテンシャルは調和的で，イオンの量子化された永年運動は量子調和振動子によって非常に正確に記述される．さらに詳細な異なる種類の Paul トラップやその諸特性については，5.3.2 項を参照してほしい．

周波数標準としては，トラップされるイオンは少なくとも一つの長い寿命で線幅の狭い遷移をもたなければならない．それは，マイクロ波（たとえば，基底状態の超微細構造遷移）または光の領域（たとえば準安定励起状態への遷移）であってもよい．ドップラーシフトや，イオンの運動と関連した他の

有害な効果を減らすには，イオンのレーザ冷却は非常に便利なツールである．この冷却機構は Wineland と Dehmelt[198] によって 1975 年に提案され，そして 1978 年に実験的に観察された [199]．基本的な量子系に関する実験と，量子論理の応用に関する実験では，必要な事項はほとんど同一である．狭い遷移はよく隔離された 2 準位系を形成する．一方，レーザ冷却は運動の調和振動子をある特定の状態に初期化するための鍵となる道具である．

5.2.6 イオンの選択とドップラー冷却

イオントラップが非常に深く（数 eV の井戸深さ），ほとんどすべてのイオンを保持できるとしても，わずかな種類のイオンだけが共振器量子電気力学のような実験に適している．それらのイオンのエネルギー準位は，自然放出の減衰によるデコヒーレンスが無視できるような 2 準位系を実現するのに適していなければならない．そして，光冷却や検出も可能でなければならない．この条件に合うイオンは典型的に最外殻に一つの電子を有し（水素型イオン），それに応じ，単純な電子準位の構造を有する．2 準位系は，二つの超微細構造基底状態によって，あるいは長寿命の準安定の電子状態によって実現できる [200]．多くの関連する実験が，$^{9}Be^{+}$ を用いて，ボルダーにある NIST のイオン蓄積グループによって行われてきた [201] が，他のグループも量子ロジックやコヒーレント制御に取り組むために準備を整えている．たとえば，IBM アルマーデン研究所 ($^{138}Ba^{+}$)，ロサンゼルスの JPL ($^{199}Hg^{+}$)[202]，ガーチング (Garching) のマックスプランク量子光学研究所 ($^{25}Mg^{+}$)[203]，ロスアラモス国立研究所 ($^{40}Ca^{+}$)[204]，マインツ大学 ($^{40}Ca^{+}$)[205]，ハンブルグ大学 [206]($^{138}Ba^{+}$, $^{171}Yb^{+}$)，そしてインスブルック大学 [207]($^{40}Ca^{+}$,$^{138}Ba^{+}$) などである．以下では，超微細構造の基底状態が 2 準位系を形成する $^{9}Be^{+}$ と，光励起された準安定状態が用いられる $^{40}Ca^{+}$ に集中して議論する．$^{40}Ca^{+}$ と $^{9}Be^{+}$ のエネルギー準位図を図 5.8 に示す．

トラップされたイオンの振動状態を，あるよく定まった状態へ初期化するには冷却が必要である．その準位として，もっとも明らかな選択は基底状態を用いることだろう [208]．しかし，トラッピング準位も提案されている [209]．運動エネルギーの大部分は，ドップラー冷却によって取りのぞくことができる．このテクニックの原理は次のような現象に基づいている．もし，レーザ光の周波数が，光学遷移周波数よりもわずかに赤方（ドップラーシフト）に離

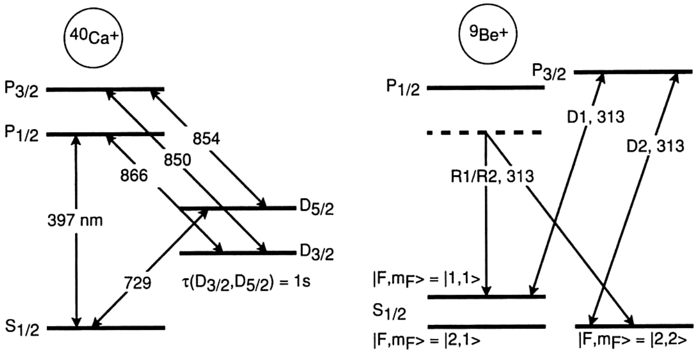


図 5.8　$^{40}Ca^+$ と $^9Be^+$ の準位図．異なる遷移に対する波長を示す．$^{40}Ca^+$ については，励起状態の寿命も示した

調されていれば，レーザ光源に対して向かっていく原子は励起されうる．光子の散乱に伴い，原子は減速する．光子の吸収に伴いイオンに受け取られる運動量は，一定して加算されていく．一方で，自然放出は 4π の立体角に広がっているため，それに伴う運動量変化の平均は 0 である．それゆえ，イオンの運動エネルギー，あるいは同じ意味だが，イオンの温度は減少する．この技術によって到達できる最終的な平均エネルギーは，ドップラー冷却限界 $E_D = \hbar\Gamma/2$ によって与えられる．ここで，Γ は冷却に用いた遷移の励起状態の自然幅である．もし，振動エネルギー（ある軸に沿った永年周波数 ω_i）が自然線幅 Γ より小さければ，同じ手順をトラップされたイオンに対しても用いることができる．この場合，必要となるレーザ光源に向かっての運動は，トラップ中でのイオンの周期的な運動によってまかなわれる．そして，自由原子の場合と同様に，この冷却プロセスの最終温度は $T_D = E_D/k_B$（典型的には，数ミリケルビンのオーダ）である [210].

たいていのイオンについて，ドップラー冷却に使用される光学遷移は紫外域にある．$^9Be^+$ については，$^2S_{1/2}$ から $^2P_{3/2}$ への 313nm の遷移が用いられ，$^{40}Ca^+$ については対応する遷移が 397nm にある．偶然の一致で，線幅は Be^+, Ca^+ の両方ともおよそ 20MHz である．冷却光は，それぞれ色素レーザまたはチタンサファイアレーザの倍波が用いられる．Ca^+ の $P_{1/2}$ 準位は，準安定状態の $D_{3/2}$ へと緩和するかもしれない．そのため，イオンを再励起するために，866nm のダイオードレーザが追加で必要になる．ドップラー冷却により，ど

ちらの場合も温度約 1mK の熱運動状態に達する．しかし，調和振動子の振動の量子の平均数に相当する量 $\langle n_D \rangle$ は，トラップの堅さ（トラッピングポテンシャルの急峻さ）に依存する．NIST で行われた Be^+ 実験で用いられたトラップでは，$\omega/2$ は 11.2MHz で，$\langle n_D \rangle \sim 1.3$ であった [211]．一方，インスブルックの Ca^+ 実験のリニアトラップのもっと弱い対称軸（$\omega/2\pi \sim 100 - 180$kHz) では，$\langle n_D \rangle \sim 50$ であった．トラップの設計は，イオン間隔と冷却方法のトレードオフによって決定される．前者は，一つひとつのイオンを単一レーザビームによって操作するのに十分大きいことが望ましく，また後者は，できるかぎり単純なものが望ましい．NIST のイオントラップが 1~2 マイクロメートルの間隔をもっているのに対して，インスブルックのイオントラップはおよそ 15 マイクロメートルのイオン間隔をもっている．

単一イオンに対しては，温度の概念はエルゴード的な意味で用いられる．つまり，繰り返された測定についての平均によって，結果的に最終のエネルギー（あるいは温度）が明らかになる．Γ より大きな振動周波数 ω_i に対しては，冷却に用いる遷移のスペクトル構造を考慮に入れることはより適当である．トラップされたイオンの振動により，吸収スペクトラムは $(\omega_0 \pm n\omega)$ に側波帯をもつ．ここで，ω_0 は遷移振動数である．これらの側波帯の強度は振動エネルギーによって与えられる．ドップラー限界以下への光冷却を得るためにこれらの側波帯を使うことができる．この方法は次節で説明されるであろう．

5.2.7 側波帯冷却

トラップされたイオンは，量子力学的な調和振動子としてよい近似で取り扱うことが可能である．図 5.9 で示されるように，一つの軸線に沿った動きに対しては，単一の 2 準位原子の内部状態は，一つの分子の構造と同様に，一つの調和振動子の準位構造によって修飾されている．そこでの振動状態は，軸線にそったトラップ振動数によって与えられる．これらの準位は，好都合なことに，内部自由度 $|e\rangle$, $|g\rangle$（電子励起を表す）と，外部自由度 $|n\rangle$（振動子の振動励起）によってラベルすることができる．列になっているイオンの場合，スペクトル構造はより複雑になる．しかし，そのようなイオン列に対しても，いくつかの変更を加えた上で，この節で概説される手順と技術の適用が可能である（5.3.3 項を見よ）．

振動の下側の側波帯において吸収が生じるようにレーザ周波数を同調することで，非常に効果的に冷却することができる．この吸収は，$|g, n\rangle \rightarrow |e, n-1\rangle$ によるものである（たとえば 図 5.9 の矢印 1）．引き続いて，搬送周波数における自然放出，すなわち $|e, n-1\rangle \rightarrow |g, n-1\rangle$（図 5.9 における矢印 2）が主に現れる．このようにして，力学的振動の平均的な励起は効果的に一つの振動量子だけ弱められる．あるいは，すみやかに緩和する第 3 の準位を介して，$|g, n-1\rangle$ へ再励起することが可能である．もし緩和での光子の反跳エネルギー E_{rec} が一つの振動のエネルギー量子よりも小さければ，振動状態は単に $E_{\mathrm{rec}}/(\hbar\omega)$ の確率で変化する．平均すると，その反跳はイオンの運動によってではなく，むしろ全体的なトラップ構造によって吸収される．これらのステップが十分な回数繰り返されると，イオンは最終的に高い確率で基底状態に残される．というのは，いったん $|g, 0\rangle$ に到達すれば，両方のレーザ場との結合が解けるからである（dark state，暗状態）．

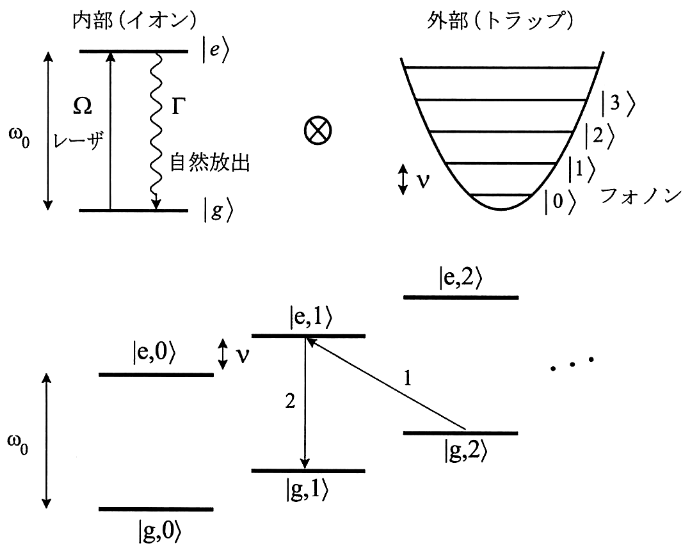


図 5.9　調和振動ポテンシャルに補足された単一 2 準位イオンの準位図．側波帯冷却は，矢印 1 で示されている $|g, n\rangle \rightarrow |e, n-1\rangle$ の遷移に伴う 1 光子吸収と，引き続いて起こる主に $|g, n-1\rangle$ への緩和（矢印 2）（自然放出あるいは追加される光ポンプ過程）によって行われる

Be^+ に対して行われた実験では，図 5.8 で R_1/R_2 として示されている，R_1, R_2 の二つのレーザビームによって誘起されるラマン遷移が，仮想的な第 3 の準位を介して，$\omega_{HF}/(2\pi) \simeq 1.25$ GHz だけ離れた二つの（超微細基底）状態を結合している．ラマンビームは，音響光学素子 (AOM) を用いて， 色素レーザの 2 倍波を $^2S_{1/2}$-$^2P_{3/2}$ から約 12GHz 離れたところに離調し，さらにそれを 1.25GHz 互いに離れた二つの成分に分けることで生成される．このようにして，二つの成分の周波数差と相対的な位相は，ラジオ周波数の正確さで制御される．レーザには高い絶対的な安定性はそれほど必要ない．NIST の実験では，およそ 1MHz の線幅をもつ色素レーザの線幅をスペクトル的に狭めるために，特別な用心はしていない．分解された側波帯冷却のために，振動数差は $\omega_{HF} - \omega$（赤方側波帯）に同調される．そして，ドップラー冷却にも使用された $^2S_{1/2}$ から $^2P_{3/2}$ への双極子遷移の励起によって誘起される再ポンピングとともに，先に述べたように冷却サイクルが行われる．

Ca^+ に対しては，自然放出寿命が約 1 秒の，図 5.8 に示されている準安定の $D_{5/2}$ と基底状態を分解側波帯冷却技術のために用いることができる．この場合もまた，狭い共鳴よりも ω だけ赤方へ離調した励起レーザによる励起を誘導することにより，運動の量子は取り去られる．ラマン遷移と対照的に，運動の側波帯を分解するために，良好な絶対的周波数安定性をレーザは示さなければならない．そのため，安定化のために注意が必要である．インスブルック大学で使われた実験では，真空中に吊され，熱的にも音響的にも絶縁された参照用共振器に対して，安定化された 729nm のチタンサファイアレーザが用いられた．その共振器のフィネスは 250000 で，予備実験はレーザ線幅が 1kHz より良いことを示唆した．反跳 (recoil) なく基底状態へと戻ることは，原則として再ポンプの手段を提供する．しかし準安定状態の寿命が 1 秒であるため，冷却は非常に遅くなる．冷却サイクルを速めるために，速く緩和する $P_{3/2}$ 準位を介して基底状態へとイオンは再ポンプされる．このような方法で，1989 年に NIST のグループは，単一の Hg^+ イオンを 1 次元について基底状態へと冷却した．Ca^+ では，再ポンプの遷移は 854nm のレーザダイオードによって駆動できる．一つのイオンの基底状態冷却，ならびに二つのイオンに対する種々の振動モードの基底状態冷却が，インスブルック大学で球状の Paul トラップにおいて観測された [215]．二つのトラップされた $^9Be^+$ イオンの運動の集団モードを基底状態へ冷却した最初の報告が，文献 [216] にある．

もしドップラー冷却により低い平均振動子量子数が得られる場合，基底状態冷却は明らかにより容易である．この場合，振動の基底状態に到達するのに，分解側波帯冷却のサイクルをほんの数回繰り返せばよい．NIST の急峻なトラップに対しては，98% の時間基底状態に到達するのには，5 回のラマン冷却サイクルで十分であった．球形のインスブルックのトラップ中の Ca^{+} の場合には，6.4 ミリ秒の冷却期間の後に，(4.5MHz のトラップ振動数において）99.9% の運動の基底状態占有が観測された．この場合，冷却レートは数 kHz であった．インスブルックの線形トラップの場合には，トラップ周波数はより低く，したがってドップラー冷却の後の振動量子数は大きくなる．このため，基底状態冷却はいっそう困難になる．しかしながら，上述したように線形トラップの利点はより広いイオン間隔である．広いイオン間隔は量子ゲート操作に対する一つひとつのイオンの番地付け（アドレシング）を簡単にする．さらに，190ms あたり 1 光子という小ささの，小さいヒーティングが観察された．これは，1.4mm と比較的大きなトラップ部分の大きさと関係している．

5.2.8　電子シェルビング法と振動の検出

少数のイオンの量子化された振動は，環境とただ非常に弱くしか結合せず，直接検出することは困難である．それと対照的に，内部の電子状態は Dehmelt[217] によって提案されたいわゆる「電子シェルビング」法によって非常に都合がよい方法で検出できる．この状況は「古典的な」共振器量子電気力学実験に非常に類似している．それらの実験では，光子場は超伝導の共振器中に閉じ込められていて，読み出すことは非常に難しい．しかし，振動子モードと相互作用した後のリュードベリ原子の測定から，間接的に類推することができる．

「電子シェルビング」法の基本的な考えは非常に単純である．基底状態 $|g\rangle$，準安定励起状態 $|e\rangle$ ，そして単寿命な励起状態 $|p\rangle$ からなる 3 準位系が必要である．基底状態はいま，励起状態 $|e\rangle$ にある一定の時間だけ結合され，結果として系はある重ね合わせ状態 $\alpha|g\rangle+\beta|e\rangle$ になったとする．$|g\rangle\rightarrow|p\rangle$ 遷移がいま駆動されたとしよう．その場合，系が $|g\rangle$ に波束が収縮したときだけに限って，短寿命の状態 $|p\rangle$ は励起されその後緩和するだろう．$|p\rangle$ が緩和する際に光子が放出され，そして原理的にはその光子は観察可能であるため，重

ね合わせに関する測定が可能である．この測定により $|\alpha|^2$ の確率で，$|p\rangle$ の励起と緩和の観測，すなわち $|g\rangle$ の結果がもたらされる．また，確率 $|\beta|^2$ で，$|p\rangle$ の励起と緩和が生じない，すなわち $|e\rangle$ の結果がもたらされる．たとえ $|p\rangle$ からの 1 回の緩和による光子の検出確率が非常に低くても（典型的には 10^{-3}），状態が $|g\rangle$ であるならば，系を再励起し続け，何百万の光子を散乱させることにより，最終的には，それらのいくつかを検出することができる．もし状態が準安定状態 $|e\rangle$ に「シェルブ（たなあげ）」されるなら，散乱は起きないだろう．どの単一の実験においても，答えは $|g\rangle$（散乱光子の検出）か $|e\rangle$（散乱光子の非検出）である．したがって，これらの状態はほぼ 100%の検出効率で測定され，そして $|g\rangle$ と $|e\rangle$ の間のすべてのコヒーレンスは破壊される．

多回数の実験を平均すれば，散乱された光子が観察される試行の数は $|\alpha|^2$ に比例するだろう．この方法の効率の例として，397nm の $S_{1/2}$ から $P_{1/2}$ の遷移を連続的に励起している間，Ca^+ イオンから散乱され光電子増倍管で検出された光を図 5.10 に示す．Ca^+ イオンが $S_{1/2}$ 状態にあるとき，それは光電子増倍管に 100 ms でおよそ 2000 個の光子を散乱する．あるとき，たとえ

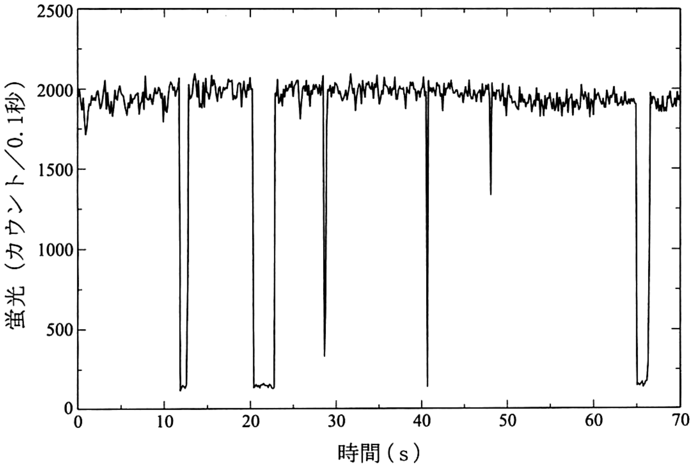


図 5.10 単一の $^{40}Ca^+$ イオンの量子跳躍．イオンが準安定状態 $D_{5/2}$ に遷移すると，蛍光量は落ちる．平均すると励起状態の寿命（$\tau \simeq 1$ s）と等しくなるようなある時間の後に，自発的な遷移によりイオンは基底状態に戻り，蛍光量は高いレベルに戻る

ば t =20 秒の付近で，イオンは 729nm の弱いビームによって $D_{5/2}$ 状態に励起され，レートは 100 ms あたり 150 回程度に落ちる．この数字は，不完全な光電子増倍管の暗計数と，397nm の励起ビームの直接散乱光が検出器に入射することによる．明らかに，二つの状態は 1 ms 以内のよい精度で区別することができる．そして，平均の暗状態の時間は約 1 秒で，それは $D_{5/2}$ 状態の輻射寿命である．

電子シェルビング法を少し変更することで，$^9Be^+$ の実験において必要となる，超微細構造の基底状態を見分けることにも応用できる．$|g\rangle$ は最大の m_F $(F=2, m_F=2)$ をもつ状態に選ばれているため，σ^+ 円偏光レーザ光（図 5.8 の D_2）を用いて，イオンを $|g\rangle$ 以外の状態へ緩和させることなく，$^2P_{3/2}$ へと繰り返しに励起できる．σ^+ 偏光の生成の実験的な不完全さと非共鳴励起の組み合わせによって，光を散乱しない状態への光ポンプが生じ，検出効率が下がる．

5.2.9　運動のコヒーレント状態

共振器量子電気力学を用いた光のコヒーレント状態の生成については 5.2.3 項で論じた．ここでわれわれは，トラップ中のイオンに対する運動のコヒーレント状態の生成について述べる．基底状態から始めて，振動周波数で共鳴する古典的な力とイオンを結びつけることによって，運動のコヒーレント状態が生成できる．最も便利な方法は，イオンを周波数 ω の駆動電場にさらすことである．駆動場の振幅，位相と継続時間に依存して，現れるコヒーレント状態は一つの複素パラメータ α によって記述される．ここで，$\bar{n}$ を平均の振動量子数として，$|\alpha|^2=\bar{n}$ である．

一つ以上のイオンに対しては，基準モードは，その共鳴周波数に調整することで励起することができる．そのとき，励起場が正しい形状をもつように注意が必要である．重心モードは一様場によって励起され，伸縮モードはある種の湾曲した場を必要とする．より高次のモードに対しては，より大きな場の運動量が必要になる．1 列のイオンの大きなコヒーレント状態 $(\bar{n}\sim 100000)$ について撮影された二つの動画を，インスブルック・グループのホームページで見ることができる．図 5.11 にも示した．この実験での場の不均一性は，最低次の二つの基準モードを励起するのに十分だった．図 5.11（左）は伸縮あるいはブリージング (breathing) モードを示し，図 5.11（右）は重心運動を示す．

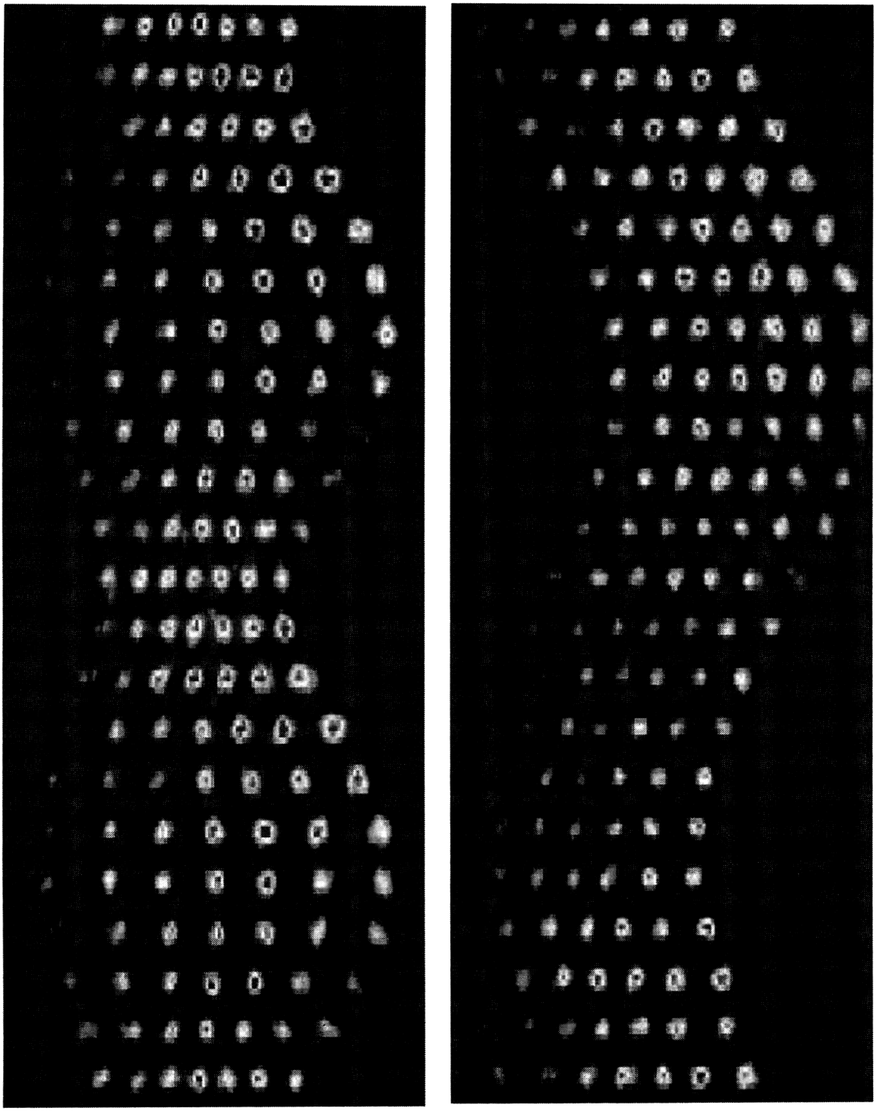


図 5.11 7 個のイオン列による（左）ブリージング (breathing) モードおよび（右） 重心運動 の実験的なデモンストレーション．図は,（振動の時間スケールと比べて短い）ある一定の時間間隔で撮ったイオン列のスナップショットをつなげたもの

画像は，低速走査の CCD カメラによってストロボ撮影のようにして撮像された．

振動モードのコヒーレントな励起に，イオンの電荷と外部電場を用いる代わりに，レーザの光場と相互作用するイオンの内部状態を用いることができる．周波数差が ω に等しい二つのレーザ（ラマン）ビームは，内部状態の遷移は引き起こさないが，より高次の振動モードをコヒーレントに励起する．結果として，二つの光場のビートによって駆動され，イオンは（集合的に）調和振動子振動数 ω で振動する．それらの二つのレーザ（ラマン）ビームは $^2S_{1/2}$ から $^2P_{1/2}$ への遷移の共鳴周波数と近いため，振動する双極子力がイオンに作用する．ラマンビームを σ^+ に偏光させることで，この力を内部状態に依存させることさえ可能である：$|g\rangle$ については，$^2P_{1/2}$ の超微細準位のうちそれと結合する状態がないため，$|e\rangle$ のみが双極子力を感じることになる．5.2.11 項で記述されるように，この点はシュレーディンガーの猫型状態を作る際非常に重要である．コヒーレント状態を生成するこれら両方の技術が，NIST グループによって単一の Be^+ イオンに対して用いられた．

小さな平均振動量子数をもつコヒーレント状態については，振動の振幅はカメラで分解するにはあまりにも小さく，イオンの運動を直接的に検出することは大変難しい．その代わりに，振動を内部の 2 準位系に結合することができる．

振動を測定する，つまり，フォノン数状態 $|\eta\rangle$ を決定するため，最初にちょうど $\delta = +\omega$ だけ青側に周波数を離調したレーザ光によって,「青側の側波帯」遷移を誘起する．$|g, n\rangle$ と $|e, n+1\rangle$ の間のこれらの遷移を図 5.12 に示す．連続発振レーザ光を用いることで， 図 5.12 で矢印によって示された準位間にラビ振動が誘発される．

青側に離調したレーザをオンにすると，もともと内部状態 $|g\rangle$ に存在するイオンが t 時間後にまだその状態に存在する確率 $P_g(t)$ は次の式で与えられる．

$$P_g(t) = \frac{1}{2}\left[1 + \sum_{n=0}^{\infty} P_n \cos\left(2\Omega_{n,n+1} t\right) e^{-\gamma_n t}\right] \tag{5.6}$$

ここで，P_n は原子を n 番めの運動数状態に見いだす確率，$\Omega_{n,n+1}$ は $|g, n\rangle$ と $|e, n+1\rangle$ の間の交換周波数である．式 (5.5) と関連して議論された限界においては，$\Omega_{n,n+1} = \Omega_0 \eta \sqrt{n+1}$ である．周波数はすべての対 $(n,\, n+1)$ に対し

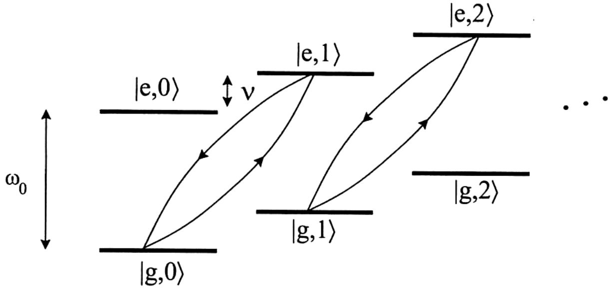


図 5.12 調和ポテンシャルに補足された単一の 2 準位イオンの準位図．矢印は，準位 $|g,n\rangle$ と $|e,n+1\rangle$ の間のラビ振動を示す．ラビ周波数は n に依存する

て異なっており，そのため $P_g(t)$ のフーリエ変換がすべての確率 P_n をもたらすということがキーポイントである．データ点は，時間 t だけ青側の側波帯輻射を照射し，前項で議論した「シェルビング」技術によってイオンの初期状態を測定することによって得られた．それぞれの時間 t に対する数多くの実験（実際には 1000 回）によって，$P_g(t)$ を推定することができる．その時間トレースから，フーリエ変換によって運動準位の確率分布 P_n を得ることができる．実験的に決定された単一の Be^+ イオンの $\overline{n}=3.1$ のコヒーレント状態に対する信号 $P_g(t)$ とそのフーリエ変換が，図 5.13 に示されている．このトレースは 図 5.2 に示されている共振器量子電気力学の結果にとても似ている．6μ 秒付近での急速な崩壊の後，信号は $t \simeq 12\mu$ 秒において復活している．信号がデコヒーレンスによって最終的に消失する前に，もう一つの崩壊と復活が 32μ 秒から 45μ 秒において見られる．

5.2.10 1 フォノン状態に対する Wigner 関数

P_n は，前項で決定されたように，密度行列 ρ の対角成分 ρ_{nn} に直接対応し，一見すると（密度行列に関して）決定できるのはこれですべてのように思われる．しかし，運動の初期状態をコヒーレントにシフトすることで，この問題を回避することができる．実験的には，まさにコヒーレント状態を生成することによりこれを行うことができる．基底状態 $|\alpha\rangle = U(\alpha)|0\rangle$ をシフトする代わりに，運動の初期状態 $|\Psi_{\rm mot},\alpha\rangle = U(\alpha)|\Psi_{\rm mot}\rangle$ がシフトされる．そして，異なるフォノン数状態 の占有 $|\langle n|U(\alpha)|\Psi_{\rm mot}\rangle|^2$ が 5.2.9 項に述べたよ

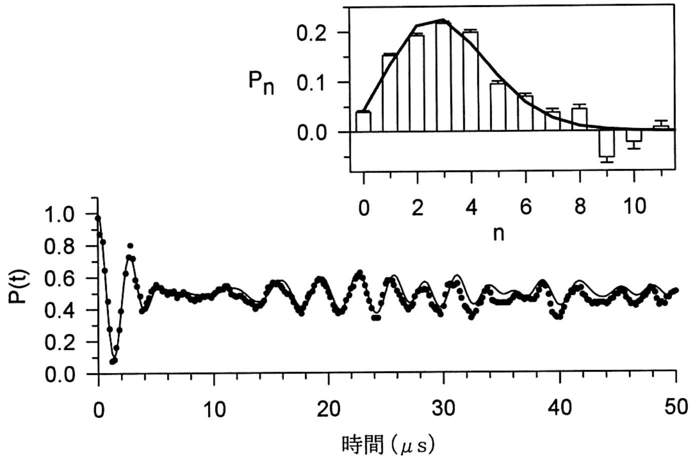


図 5.13　コヒーレント状態に対する P_g. 実線は，データ（点）を，コヒーレント状態の分布をもつ個数状態の合計にフィットしたもの．フィットにより得られた平均量子数は $\overline{n}=3.1\pm0.1$. 挿入図は，個数状態の成分の振幅（棒）と，$\overline{n}=2.9\pm0.1$ に対応するポアソン分布へのフィット（実線）. (文献 [220] から再構成した)

うに測定される．十分な数のシフトパラメータ α とともに，個数状態基底での密度行列の非対角要素，あるいは運動の初期状態の Wigner 関数 [219] を再構築することができる．

運動の基底状態から始めて，式 (5.5) で与えられるハミルトニアンによって提供される手の内の手段によって，運動状態をほとんど思うがままに作ることができる．実際，NIST のグループにより，熱状態，個数（フォック）状態，スクィーズド状態，シュレーディンガーの猫型や他の個数状態の重ね合わせ状態のすべてが単一イオンについて生成され解析された [219]-[221].

個数状態は，青側と赤側の側波帯に対する相補的な π パルス列によって基底状態から生成される．このパルス列はイオンに次の梯子を登らせる：$|g,0\rangle \to |e,1\rangle \to |g,2\rangle \to \cdots$ など．このようにして，最大 $n=16$ の個数状態が生成される．これらの $P_g(t)$ の信号は，その周波数が大まかに $\sqrt{n+1}$ に比例して増加し，η がゼロでない ($\eta=0.202$, [220] の図 1 を見よ) ことからくる偏差をもつ，単純な sin 関数である．いっそうおもしろいのは，n が奇数であるとき個数状態に対して負の領域をもつ，Wigner 関数である．実験的に決定された

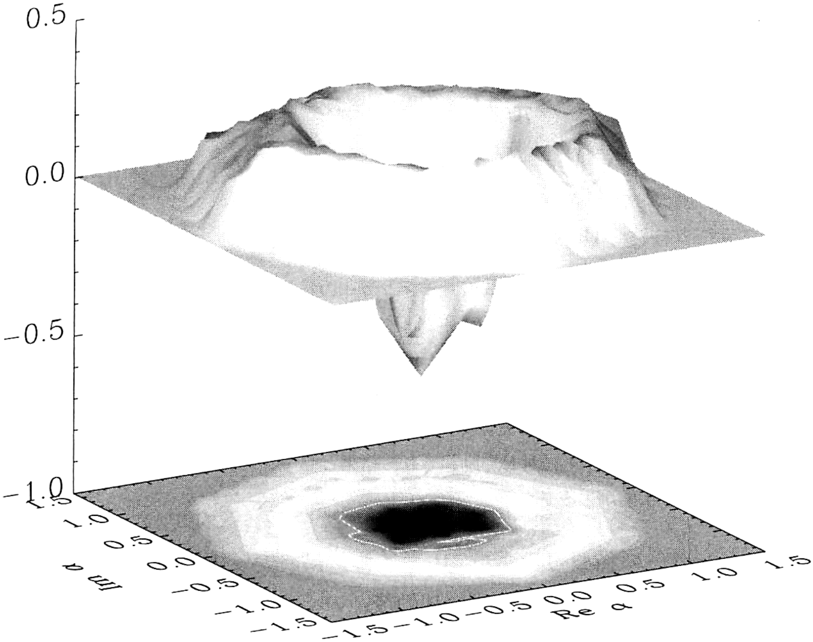


図 5.14 約 $n = 1$ の個数状態の Wigner 関数 $W(\alpha)$ の表面プロットと等高線プロット．中心付近で $W(\alpha)$ の値が負になっており，この状態が非古典的であることを際立たせている．(文献 [219] から再構成した)

$|n\rangle = |1\rangle$ に対する Wigner 関数が，図 5.14 に示されている．実験的に決定された Wigner 関数は原点の周りで負になっており，理論とよく一致している．

5.2.11 イオンのスクィーズド状態とシュレーディンガーの猫状態

電場あるいは適当に離調された 2 本のラマンビームによって，イオンを 2ω で駆動することで，光パラメトリック発振器と同様に真空スクィーズド状態を作り出すことができる．直交位相の比率 40（スクィーズされた直交位相で 16 dB の雑音抑圧）の真空スクィーズド状態が実験的に作られた．残念なことにスクィーズド光と対照的に，この驚くほどのスクィージングを利用可能な高感度な測定への応用はいまのところ存在しない．

光子場の代わりにイオンの振動で置き換えられた式 (5.4) と正確に同じ形のシ

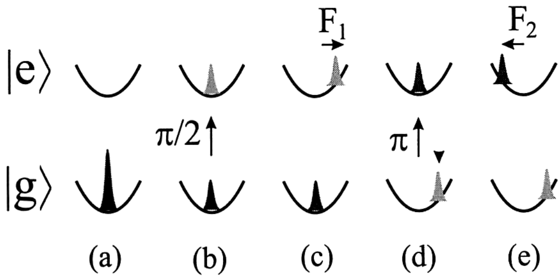


図 5.15　イオンを用いたシュレーディンガーの猫状態の生成．(a) 初期状態 $|g, n = 0\rangle$．(b) $\pi/2$ −パルスによって $|g, 0\rangle$ と $|e, 0\rangle$ の重ね合わせ状態が作られる．(c) 偏光したラマン光線と $|e\rangle$ の間の相互作用による振動のコヒーレント状態の励起．(d) π-パルスにより内部状態の分布が入れ替わる．(e) 最後に，もう一つのコヒーレント状態が $|e\rangle$ に対して励起され，結果としてシュレーディンガーの猫状態が生成される

ュレーディンガーの猫型の状態が，Be^+ イオンにおいて生成された．図 5.15(a) に表される $|g, n = 0\rangle$ へのレーザ冷却の後，いくつかの連続的なラマンビームパルスを適用することによって，シュレーディンガーの猫状態は作られる．

搬送周波数の $\pi/2$ パルスが波動関数を，図 5.15(b) で示されるような状態 $|g, 0\rangle$ と $|e, 0\rangle$ の等しい重ね合わせ状態に分ける．そして，相対的に ω だけ離調された偏光ラマンビームが，$|e\rangle$ 成分と相関する運動成分だけを，5.2.9 項で説明し，また図 5.15(c) に示すようにコヒーレント状態 $|\alpha\rangle$ へと励起する．図 5.15(d) は，搬送周波数の π パルスが，重ね合わせにある内部状態をどのように交換するかを図示している．図 5.15(e) は，2 番めの偏光ラマンビームパルスが，新たな $|e\rangle$ 状態を第 2 のコヒーレント状態 $|\alpha e^{i\phi}\rangle$ へと励起する様子を示す．この手順の後，状態は望んでいた次の形式をもつ．

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|e\rangle|\alpha e^{i\phi}\rangle + |g\rangle|\alpha e^{-i\phi}\rangle\right) \tag{5.7}$$

相対的な位相 ϕ はラマンビームの rf 差周波数の位相によって決まる．その位相は，rf 源の位相を固定することで容易に制御できる．この状態のデコヒーレンスの特性を調べる場合，(振動モードは）共振器モードの減衰ほどはモデル化も特徴づけもされていないという欠点を抱えなければならない．その一方で，可能である多様な相互作用は実験家に熱浴を思いのままに設計するこ

とを可能にするかもしれない [222]．もたらされる散逸の時間スケールが，この人工的な熱浴がないときに観察される散逸よりはるかに短いようにカップリングが調整される限り，この熱浴は系のデコヒーレンスを大きく決定するだろう．

5.2.12 捕捉された単一の ^{9}Be$^+$ イオンによる量子ロジック

4.3 節で述べたように，レーザ場と相互に作用している捕捉された冷却イオンは，量子ゲートの実験的な実現のための強力な候補である．これは最初に Cirac と Zoller によって指摘された [156]．量子情報はそれぞれのイオンの内部準位からなる量子ビットに蓄えられる．一方，運動の基準モードは，トラップ中のイオンによって共有され，エンタングルメント状態を生み出すための「データバス」として用いられる（5.3.7 項を参照）．二つのイオンを運動の基底状態まで冷却することも達成され，さらに多くのイオンを含む列に対して基底状態冷却の実現に向けた進展が続けられている．

1995 年に行われた実験で， NIST グループは一つのイオンの二つの内部状態（$|g\rangle$ と $|e\rangle$ ，標的ビット）と，そのトラップ中の運動 ($|n=0\rangle$ と $|n=1\rangle$, 制御ビット）の間での，量子制御 NOT ゲートを実現した．つまり,「データバス」から調和振動を読み出せることを示したわけである [223]．一連の三つのレーザパルスが，ゲート操作を行うために照射された．

1. 搬送周波数の $\pi/2$ パルスが，$|g\rangle$ と $|e\rangle$ の重ね合わせ状態を作り出す．
2. $|e\rangle$ と $|aux\rangle$ を結ぶ補助的な遷移に対応する青側の側波帯について，2π パルスを適用すると，重ね合わせ状態の $|e\rangle$ 部分について条件付きの位相シフトが生じる．もし振動が $|n=1\rangle$ であれば，この側波帯は $|e\rangle$ と $|aux\rangle$ のみを結合するため，$|e\rangle$ 部分の位相は反転する．
3. 最後に，搬送周波数の $\pi/2$ パルスが，状態の同位相あるいは逆位相での干渉を引き起こす．それは，$|e\rangle$ 部分で，条件付き位相シフトが得られたかどうかに依存する．

いっそう直観的な描像を得るには，この全体の手順を，共鳴周波数での一つのラムゼイ実験と考えればよい．$|g\rangle$ から始まり，最初の $\pi/2$ パルスによって，$|g\rangle+|e\rangle$ の重ね合わせ状態が生成される．そして，n =0 かどうかに依存して，重ね合わせ状態はそのままにされるか，あるいは励起部分に位相シフ

トが導入される.（つまり，$n=1$ のときに限り $|g\rangle - |e\rangle$ ）. 最後のステップは $-\pi/2$ パルスである．このとき，位相シフトがなければ内部状態は $|g\rangle$ に戻るが，もし位相シフトが起こっていれば $(n=1)$，$|e\rangle$ へと反転するだろう．制御量子ビットはこのプロセスの間，変化せずにいる．NIST グループはこのようにして実行された制御 NOT 操作に対して真理値表を測定し，そしてまたゲートのコヒーレンスを証明した（文献 [223] の図 2 および図 3 を参照）.

5.2.13　比較と展望

これまでの節で，共振器量子電気力学とイオントラップに基づいた量子情報ならびに量子計算の実験を記述した．たとえ共振器量子電気力学とイオントラップ実験が基本的にジェインズ–カミングス型のハミルトニアンを実行し，それゆえ同様のダイナミクスであるとしても，それぞれの技術が独自の強みと欠点をもっている．二つの技術の間の本質的な相違をこの項で示す.

初期状態の準備はマイクロ波共振器量子電気力学に対する標準的な技術を必要とする．共振器の基底状態は，^{3}He 温度への低温（クライオスタットを用いた）冷却によっておそらく達せられるだろう．長寿命の円形リュードベリ原子の速度選択されたビームの生成には，いくつかの標準的な赤外線のダイオードレーザとラジオ周波数の電場が必要になる．イオンのレーザ冷却はたいてい紫外光源を必要とする．共振器量子電気力学実験はジェインズ–カミングス相互作用を厳密に実現するが，トラップ中のイオンに対するカップリングは，ラム–ディッケ・パラメータが小さい限界におけるジェインズ–カミングス・ハミルトニアンの近似に過ぎない．他方，振動モードとの捕捉されたイオンのカップリングは，基本的なジェインズ–カミングス相互作用に比べて，より多くの自由度をもたらし，またより洗練された機能を実現するためにそれらの自由度を思うがままに制御することができる．原子 / イオンのデコヒーレンスは，原子のリュードベリ状態ならびにイオンの 超微細 / 準安定状態の双方に対してほとんど無視できる．調和振動子のモードについては，超伝導共振器の損失はかなりよく理解されて，そしてモデル化できる．唯一のデコヒーレンスの調整可能なパラメータ，共振器の Q 値は古典のマイクロ波技術によって独立して決定される．捕捉されたイオンについては，振動のデコヒーレンスの原因はまだよく解っていない．デコヒーレンスの「基本的な」原因，たとえば電極構造内に誘起されるイオンの鏡像電荷や背景ガスの

衝突についての計算結果は，実験的に観測される値よりも一桁以上も低い加熱レートになる [215,218]．この「異常な」加熱は，それらについては基本的な理由が知られていないので，さらなる研究により克服できるかもしれない．

量子情報について興味深い操作を行うためには，少なくとも少数の量子ビットを操作することが必要になる．現在の技術を用いた，共振器を横切る円形のリュードベリ原子ビームに依存する共振器量子電気力学実験は，連続する原子が二つか三つ以上になると非常に難しいことがわかる．先に議論したように，2 原子のイベントを避けるために，パルスごとの平均原子数は 1 よりも十分に下げなければならない．そのため，三つあるいは四つの原子の一致（コインシデンス）は非常にまれで，計測時間は原子の数に対して幾何級数的に増加する．この限界はイオントラップの実験には無関係である．少数のイオンを線形トラップで捕えることは比較的容易である．個別によく焦点を合わせられたレーザパルスによって個々のイオンを扱うことも可能である．イオンの集団が振動の基底状態まで冷却されるなら，少数の量子ビットに対する量子論理操作は実現可能だろう．

もう一つのイオントラップ実験の主要な強みは，量子シェルビング法を用いて，イオンの状態をほとんど100%の量子効率で検出可能であることだ．たとえば，ベルの不等式を検証する実験をエンタングルメント状態にある捕捉されたイオンによって行うとすれば，非常に容易に「検出効率の抜け穴」を塞いだ実験を行うことができるだろう．しかし，光子やさらに原子を用いた実験では，その抜け穴はまだ塞がれていない（共振器量子電気力学では，検出効率を 90%よりさらに高くすることはほとんど望みがない）．

このように,「古典的な」共振器量子電気力学の実験は，非常によく制御された系のなかでの，限られた数（最大約 4）の原子に対する，デコヒーレンスやエンタングルメントの研究に適しているように思われる．GHZ タイプでエンタングルメントした三つの原子の生成実験が現在行われている．デコヒーレンスに関するさらなる研究も行われてゆくだろう．特に，直接共振器場の Wigner 関数を決定することが可能である [224]．これはシュレーディンガーの猫状態のデコヒーレンスをより深く理解することを許すだろう．最後に，二つの離れた超伝導共振器による実験は，非局所的なメゾスコピック状態という量子世界の二つの最も興味をそそる特徴を結合できるだろう．

イオントラップでは， Wigner 関数の再構築はすでに実証された．しかし，

理論モデルの欠如とイオントラップの中のデコヒーレンスプロセスの性質が不明なことが，その理解を困難にしている．イオントラップはまた，中程度の規模について量子論理を研究する手段として有望である．その規模は，おそらく 1 ダースの量子ビットと，数百の操作に達するだろう．しかしながら，Shor の因数分解アルゴリズム (4.2 節を参照）を，古典暗号を解読するために必要な「興味深い」数に対して実行するには，最低でも 400 量子ビットが必要になる．これは，現在の知識と技術では届きそうにない [225].

たとえば自然放出のような，基本的な限界をうち破るために，新しい方法が発見される必要がある．しかし，エラー訂正とコードの安定化技術（第 7 章）は，これらの問題に対して取り組む方法を提供するかもしれない．その途中においても，少数の量子ビットによって取り組むことが可能な多くのおもしろい量子情報処理の操作がある．たとえば，エンタングルメントの精製 (entanglement purification) などである．これらの「豊かな情報を含む」状態は，イオントラップを用いた周波数標準の性能を改善するために使うことができるかもしれない（7.6 節）.

それらさまざまな応用可能性以上に，よく制御された環境中で相互作用する単純で基本的な系に関する実験により，量子力学のもっとも奥にある特徴をわれわれはつかむことができるだろう．

5.3　量子計算のための線形イオントラップ

(*H.C. Nägerl, F. Schmidt-Kaler, J. Eschner, R. Blatt, W. Lange, H. Baldauf, H. Walther*)

5.3.1　はじめに

5.2 節で述べたように，単一イオンの量子状態がほぼ完璧に制御できれば，次の興味は相互作用がよく制御された複数のイオンを含む系に移行する [226]. 複数イオンの量子状態を操作することには，古典系では実現できないエンタングル状態をつくることが含まれる．イオンのように大きな粒子のエンタングル状態がつくれれば，量子力学を検証するためのベル状態と GHZ 状態に関する測定といったまったく新しい実験の可能性もひろがる [176]．さらに，

粒子のエンタングルメントは，量子測定のプロセスやデコヒーレンスに関する新しい研究も可能にする [183, 221].

量子コンピュータの基本要素である量子演算ゲートを実現するために，一列に捕捉（トラップ）されたイオンの鎖を利用することが提案された [156]. 素子は，量子ビットの集合体である量子レジスタで動作するが，それらの量子ビットは古典的なビットと同様にゲートによって操作される．イオントラップ演算は，イオンの内部自由度（電子励起）とイオン鎖の集団的運動（振動励起）により多数の量子ビットが論理的に統合されることによって実現する．量子計算における制御 NOT ゲートは古典計算における XOR ゲートに相当するが，これは波長が制御されたレーザパルスの系列をイオン鎖中の異なる二つのイオンに照射することによって実現する．制御 NOT ゲートは万能量子ゲートであることが示されたため，すべての量子演算がこの 2 ビットの制御 NOT 量子演算と 1 ビットの回転の組み合わせで実現する [227]. これらの 2 種類の演算をイオン鎖で実現することが基本的な興味である．なぜなら，すべての基本的な量子アルゴリズムがトラップされたイオン鎖で試すことができるようになるからである．

本節の目的は, 線形イオントラップの特徴的な性質をまとめ，それらの量子計算への応用を議論することにある．5.3.2 項にはイオントラップに基づく演算と，線形トラップを実現するためのさまざまな手法を示す．5.3.3 項ではイオン鎖を用いた量子演算の初期化に必要な基底運動状態への冷却について述べる．5.3.4 項ではイオンの並び方を含む構造に関する議論を簡単に行う．5.3.5 項から 5.3.9 項では，状態の準備と操作， 協調的なモード励起，そして内部電子状態の読み出しといった量子ゲートの基本動作を実現するための具体的な手法を紹介し議論する．

5.3.2 線形 Paul トラップへのイオン閉じ込め

イオン化した原子のような荷電粒子は，静電場と磁場の組み合わせ（Penning トラップ）や，時間に依存した不均一電場（Paul トラップ）といった電磁場によって閉じ込めることができる [197]. 捕捉されたイオンを量子ビットやレジスタとする場合は，Paul トラップとその線形化がもっとも適していると考えられる [228].

一つの粒子を閉じ込めるためには，たとえば $\boldsymbol{F} \propto -r$（$r$ は捕捉中心からの

距離）に代表される復元力 $\boldsymbol{F}$ が必要となる．そのような力は 4 重極子ポテンシャル $\Phi = \Phi_0(\alpha x^2 + \beta y^2 + \gamma z^2)/r_0^2$ で与えられる．ここで Φ_0 は 4 重極子に印加された電圧，r_0 は特徴的なトラップの大きさで，定数 α, β, γ はポテンシャルの形を決定する．たとえば，Paul トラップにおける 3 次元空間での閉じ込めは $\alpha = \beta = -2\gamma$ という条件で実現されるが，$\alpha = -\beta, \gamma = 0$ の場合は 4 重極子による質量フィルタとなる．Paul トラップは，3 次元空間中の 1 点に対する復元力を提供するため，単一イオン実験や，1 点を中心とした多数イオンの閉じ込め実験に利用された．一方，量子レジスタを捕捉されたイオンで実現するためには一直線に並んだイオン（イオン鎖）が必要となる．よって 4 重極子質量フィルタのポテンシャルに基づく Paul トラップの線形化に注目が集まるようになった．後者のポテンシャルは z 軸に垂直な 2 次元面内に対する閉じ込め力を提供するが，z 軸に平行な運動には変化を及ぼさないため，軸方向の閉じ込めには，新たに電極を設ける必要がある．軸を中心とした半径方向の閉じ込めは電極に直流電圧 U_{dc} と交流電圧 $V_{\mathrm{ac}} \cos(\Omega t)$ を印加することで実現できる．これによって捕捉軸の近傍では以下のポテンシャルが形成される．

$$\Phi = \frac{U_{dc} + V_{ac}\cos(\Omega t)}{2r_0^2}(x^2 - y^2) \tag{5.8}$$

ここで r_0 は一つの電極の表面から捕捉軸への距離である．もし直流電圧のみが印加された場合は，図 5.16 に示すとおりの一方向のみに閉じ込めが生じるポテンシャルとなってしまう．しかし時間に依存する交流電圧が印加されれば捕捉が得られる．実際に図 5.16 では, 電圧の正負を反転させることにより, 反転前には不安定であった方向への閉じ込めが得られている．

ここでは周波数 Ω を的確に選ぶことが重要となる．式 (5.8) から推測できるとおり, 理想的にはポテンシャルは双曲線形の電極によって形成される（図 5.17(a)）. 実際の電極は，レーザの導入方法やその他の技術的な要求によって，図 5.17(b) に示す円柱型や図 5.17(c) のさらに工夫された形状で置き換えられる．半径方向の閉じ込めは，図 5.17(b) に示すリング状電極や，図 5.17(c) に示す分割された棒電極によって得られる z 軸方向の静的ポテンシャル U_{cap} によって達成される．すなわち，縦方向の閉じ込め周波数によって特徴づけ

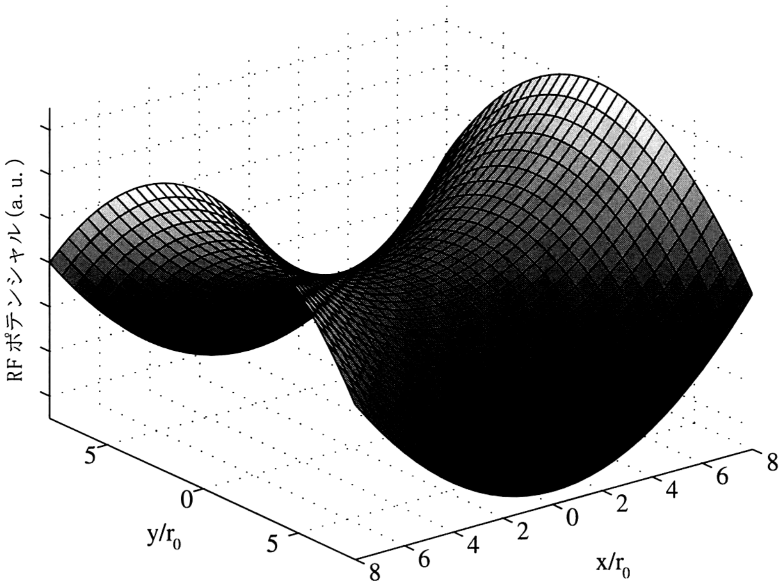


図 **5.16** 高周波 Paul トラップの鞍型ポテンシャル．$x = y = 0$ 付近の荷電粒子の閉じ込めはポテンシャルの符号を急速に変化させることによって得られる

られる z 方向の静的放物ポテンシャル

$$\omega_z = \sqrt{2\kappa q U_{\rm cap}/m z_0^2} \tag{5.9}$$

が形成される．ここで m と q はイオンの質量と電荷，z_0 は半径方向に閉じ込めるための電極間の距離の半分，κ は特定の電極配置に対する形状的補正でオーダとして 1 の値を有する．原理的には κ の正確な値は数値計算または解析的に求められる．しかし，実験データをモデル化するためには，実際に測定された κ の値を利用することが十分かつ現実的である場合が多い．式 (5.8) による x と y 方向の運動は，次の Mathieu の方程式によって与えられる [228].

$$\frac{d^2 u_x}{d\tau^2} + (a_x + 2q_x \cos(2\tau))u_x = 0 \tag{5.10}$$

$$\frac{d^2 u_y}{d\tau^2} + (a_y + 2q_y \cos(2\tau))u_y = 0 \tag{5.11}$$

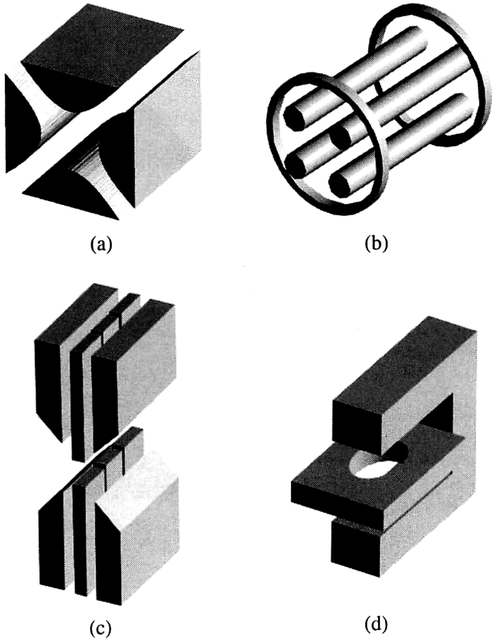


図 5.17　線形イオントラップのさまざまな形態. (a) 線形4重極型トラップ; (b) 四円柱電極型トラップ; (c) 線形終端キャップ型トラップ; (d) 楕円リング付き Paul トラップ

ただし

$$a_x = \frac{4q}{m\Omega^2}\left(\frac{U_{\mathrm{dc}}}{r_0^2} - \frac{\kappa U_{\mathrm{cap}}}{z_0^2}\right) \tag{5.12}$$

$$a_y = -\frac{4q}{m\Omega^2}\left(\frac{U_{\mathrm{dc}}}{r_0^2} + \frac{\kappa U_{\mathrm{cap}}}{z_0^2}\right) \tag{5.13}$$

$$q_x = -q_y = \frac{2qV_{\mathrm{ac}}}{m\Omega^2 r_0^2} \tag{5.14}$$

$$\tau = \frac{\Omega t}{2} \tag{5.15}$$

式 (5.10), 式 (5.11) の一般解は，捕捉周波数 Ω を有する無限級数の調和振動として与えられる [197]. 通常は $a_1 < q_i^2 \ll 1, i = x, y$ という条件が満たされ，運動方程式に対する近似解が得られる．これは周波数 ω_i における巨視的な調和永年運動と，トラップの駆動周波数 Ω を有する微視的運動の重ね合わせと

なる．

$$u_i(t) = A_i \cos(\omega_i t + \varphi_i)[1 + \frac{q_i}{2}\cos(\Omega t)], \qquad i = x, y \tag{5.16}$$

振幅 A_i と位相 φ_i は初期条件に依存し，永年周波数は

$$\omega_i = \beta_i \frac{\Omega}{2}, \qquad \beta_i \approx [a_i + \frac{q_i^2}{2}] \tag{5.17}$$

で与えられる．この極限で通常の $U_{\mathrm{dc}} = 0$ を適用すると，微視的運動は無視できるほど小さく，閉じ込められたイオンは以下の半径方向の擬調和ポテンシャル Ψ に捕捉された状態で振動する．

$$q\Psi = q\frac{|\nabla\Phi|^2}{4m\Omega^2} = \frac{1}{2}m\omega_r^2(x^2 + y^2) \tag{5.18}$$

ここで $\omega_r \approx qV_{\mathrm{ac}}/(\sqrt{2}m\Omega r_0^2)$ は半径方向の永年周波数である．

単一のイオンを捕捉する 3 次元の Paul トラップと比較した場合，線形 Paul トラップの大きな利点は，z 軸に閉じ込められたイオンの微視的運動が完全に消滅することである．よって，イオンの運動は，半径方向の静的ポテンシャルに基づく純粋な調和振動となる．

イオンの線形トラップを量子レジスタとして用いることが望ましいが，3 次元 Paul トラップを一方向に引き伸ばした方法でも 2〜3 個のイオン鎖を得ることができる [216]. 図 5.17(d) に示すとおり，1 個の楕円形リング電極と 2 個の終端型電極を含むこの構成では，イオン鎖は楕円電極の長軸にそって形成される．この配置では線形トラップと比較して非常に高い周波数での動作が可能で，このことは光学的冷却に向けて有利である（5.2.7 項と 5.3.3 項を参照）．一方，微小ではあるが残留運動が常に残る欠点もあり，このことはイオン鎖の高周波 (rf) 加熱につながる．

5.3.3 レーザ冷却と量子運動

量子情報を正確に保持するためには，イオン鎖を構成する各イオンの量子状態が入念に準備されることが必要である．これには 5.2.7 項で単一イオンに適用されたような，レーザ冷却技術が利用される．冷却の最終段階にはサイドバンド冷却技術が用いられ，イオン鎖の運動は基底状態に落ち着く．ただし，鎖特有の振動モードが単一イオンとは異なる周波数をもつために冷却プロセスは多少変化する．5.2.7 項で説明した単一イオンのサイドバンド冷却

法は，2 個以上のイオンには適用できない．重要な違いは，単一イオンでは等間隔の離散的エネルギー準位が形成されたのに対し，鎖では協調的運動に起因する不整合な振動モードが擬連続的なエネルギー準位を形成する点である．よって系のエネルギー準位は，内部状態（$|g\rangle$ または $|e\rangle$）と運動状態 ($|\boldsymbol{n}\rangle$) によって表される．ここで，$\boldsymbol{n} = (n_1, n_2, \cdots)$ は $\omega = (\omega_1, \omega_2, \cdots)$ の周波数を有する運動モードの量子数ベクトルによって記述される．これに対応して $|g, \boldsymbol{n}\rangle$ から $|e, \boldsymbol{m}\rangle$ への共鳴遷移のスペクトルは，単一イオンの場合と比較して，はるかに高い密度のサイドバンドを有する．よって，レーザの周波数をある特定の値に設定すると，その周波数周辺のレーザ線幅 γ に存在するすべてのサイドバンド遷移が同時に励起される．

さらに厳密に考えるには，2 種類の場合分けが必要である [229]．運動状態 n_j と $n_{j\pm1}$ が光によって結合されたラム－ディッケ領域では，1 次のサイドバンドのみが寄与し，複数の振動量子状態の交換は抑制される．サイドバンドのスペクトルは図 5.18(a) に示すとおりシンプルで，単一イオンの場合のように，一つのサイドバンドに周波数を合わせることで，そのサイドバンドに対応するモードが冷却される．しかし，その状況は単一イオンの場合と完全

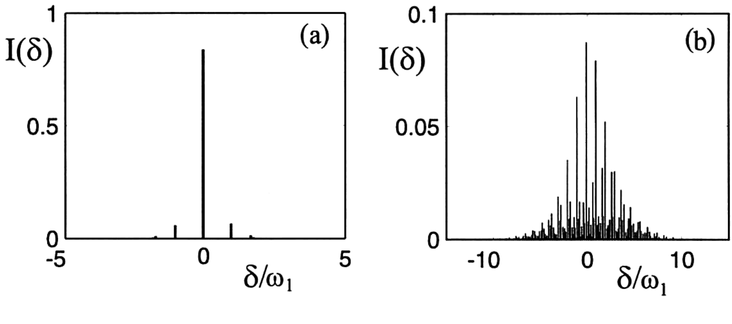


図 5.18　二つの捕捉されたイオンの共鳴スペクトルで，ラム－ディッケ領域の (a) 内と (b) 外の場合の比較．光学遷移に関して，原子の運動状態が変化しない離調なしのピークと，運動状態の変化に起因する特定の離調に対応するサイドバンドピークが示してある．ラム－ディッケ領域内 (a) では，1 個の振動量子の交換による $\delta = \omega_{1,2}$ の基本的なサイドバンドのみが重要となる．ラム－ディッケ領域外 (b) では電子状態と振動状態が変化した結果の多くのサイドバンドが出現する．図は文献 [229] より引用した

に一致するわけではない．レーザと相互作用をもたない他のモードが自然放出によって発熱するため，単一イオンの場合よりレーザ周波数設定に幅をもたせ，はるかに広い線幅 γ の光を当てることが基底状態を得るためには必要となる．

一方，現在の線形イオントラップの量子演算では，ラム－ディッケ領域外でサイドバンド冷却を行う．図 5.18(b) に，この場合の 2 個のイオン鎖に対するサイドバンドスペクトルを示す．レーザの周波数が共振周波数より小さく設定された場合，それによって誘発される遷移は両モードの 1 個以上の量子数変化を伴う．この場合は，ラム－ディッケ領域内とは異なり，両モードともに同時に冷却される．さらに，冷却速度のレーザ周波数幅 γ 依存性も異なる．冷却速度は周波数幅の増加とともに非線形的に増加するが，その第 1 の理由は吸収と放出の周期が線幅に比例することで，第 2 の理由が初期状態が利用できる準位数，すなわち冷却に利用できるチャンネルの数が線幅 γ とともに増加することである．もし，ドップラー冷却の後でも多くの振動量子が励起されているとすれば，冷却速度（冷却にかかる総時間）を考慮することが非常に大切となる．これが線形イオントラップにおける典型的状況である．

数値計算は，ラム－ディッケ領域内と領域外の両方においてサイドバンド冷却が適用でき，2 個のイオンの運動が基底状態に導かれることを示した [229]．ラム－ディッケ領域外では，冷却速度の強い線幅 γ 依存性を利用して冷却時間が最適化できる．

冷却に用いるイオンは，必ずしも量子計算に用いるイオンと同様である必要はない．ガーチング (Garching) のマックス・プランク量子光学研究所では，マグネシウムとインジウムを含む線形鎖を用いた実験に成功した．インジウムはサイドバンドによって大変効率的に冷却され [230], マグネシウムは量子情報の担い手として利用された．冷却と計算を分離することで，すべての標準振動モードの連続冷却が量子レジスタの情報を乱すことなく達成できる．

Paul トラップにおける基底振動状態へのレーザ冷却に関してもう一つ重要となるのが，残留もれ電界の入念な補償である．そのような電界は電極上の不均一な電界によって生じ，イオンを捕捉中心から押し出し微小な残留振動を誘発する原因となる．その結果として光学的冷却を妨げることもある．もれ電界は，そのために新たに追加された電極群に直流電界を印加することにより補償され，イオンは捕捉中心に押し戻される．これは通常の Paul トラッ

プ中の 3 次元空間において定常的に用いられる手法であり，似たような方法が線形イオントラップにも適用できる．イオンの一連鎖の場合，注意深い電極の配置こそが微小振動の補償にむけて重要となる．

5.3.4　イオン鎖と標準モード

線形イオントラップでは，イオンを規則的な構造をもつように閉じ込め，光学的に冷却することができる [212,231]．もし半径方向の閉じ込めが十分に強ければ，イオンは一直線に並び，その間隔はイオン間のクーロン反発と半径方向の閉じ込めポテンシャルの熱平衡状態によって決まる．図 5.19 に Ca^+ イオンの一連鎖を例として示す．

イオンの熱平衡位置は数値計算によって計算できる．半径方向の閉じ込めポテンシャルが十分に調和的であれば，イオン位置は式 (5.9) の軸周波数 ω_z で表せる [212,232]．ただし，イオン間にクーロン相互作用があるため，平衡状態から微小にずれた状態の各イオンの位置を，それぞれが独立した状態として表すことはできない．すなわち，イオン鎖全体が特定の周波数を有する標準モードで振動していることを前提に，イオン鎖の運動を表記する必要がある [156,232]．その例として 2 個のイオンが線形トラップに閉じ込められた場合を考えよう．最初の標準モードでは，二つのイオン間の距離は棒でつながれたように一定に保たれ，それら 2 個が同時に軸にそって振動する．この振動は鎖の重心モード (COM) と呼ばれる [232]．二つめの標準モードは，二つのイオンが反対方向に振動する場合に相当する．これは伸縮モードとして

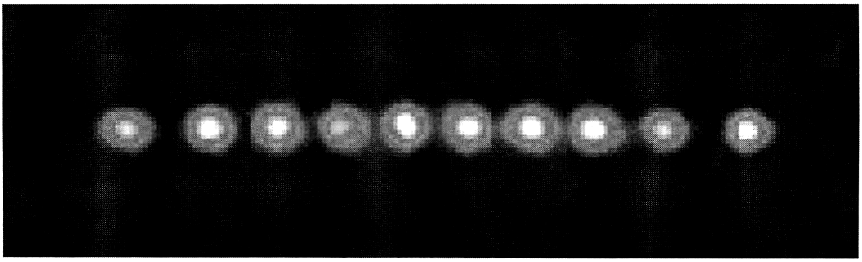


図 **5.19**　線形 Paul トラップ中のイオン鎖の例．近接したイオン間の平均距離は約 10μm．CCD カメラの露光時間は 1 秒．レンズと CCD カメラから構成される画像化システムの空間分解能は 4 μm 以下．文献 [231] と比較するとよい

知られ，N 個の一連鎖の振幅が捕捉中心からの距離に比例している場合に相当する．5.2.9 項の図 5.11(a) と (b) がインスブルック大学で観測された 7 個のイオン鎖の重心モードと伸縮モードのストロボ写真である．

標準モード（固有モード）とそれらの固有振動数の正確な計算は以下に述べるシンプルな結論を導く [200,232]: (i) N 個のイオンから形成される 1 次元鎖では，正確に N 個の標準モードと標準周波数が存在する．(ii) 重心モードの周波数は単一イオンの周波数と正確に等しい．(iii) 高次モードの周波数はイオン数 N にほとんど依存せず，(1, 1.732, 2.4, 3.05(2), 3.67(2), 4.28(2), 4.88(2), $\cdots$) ω_z によって与えられる．ただし，カッコ内の数字はイオン数 N が 1 個から 10 個に増やされた場合の最大変化量を示す．(iv) 少なくとも 4 個以上のイオンを含む鎖に対しては，標準モードの相対的振幅は数値的に解析しなければならない（文献 [232] の式 (28) を参照）．トラップでイオンの一連鎖を形成した後，リング電極か補償用電極に交流電圧を印加することにより標準モードが励起される [212]. 励起された標準モードは，光倍増管の蛍光シグナル強度の低下が生じるまで，CCD カメラ上のスポット幅の増加という形で観測される．測定された伸縮モードの周波数は，1%という大変正確な範囲で，理論が予想する重心周波数の $\sqrt{3}$ 倍と一致する．図 5.20 には 5 個イオンの鎖に対して，2 種類の振幅に関する重心モード (158.5 kHz) の励起と，伸

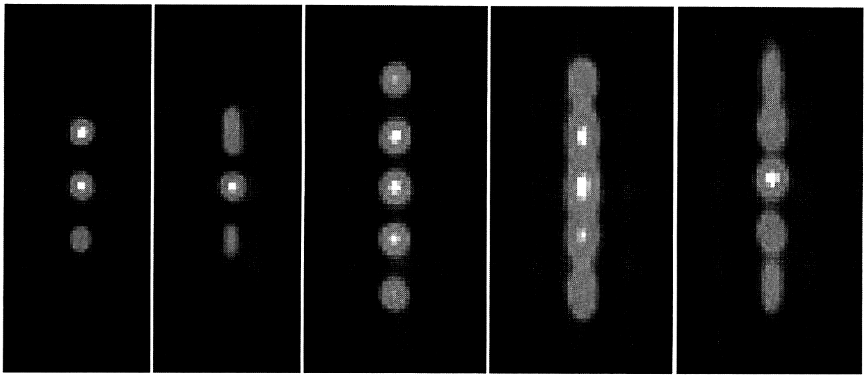


図 5.20 外部から交流電圧を印加することで励起される 5 イオン鎖の振動モード．左から：励起なし，重心モード (158.5 kHz) の弱い励起，重心モード (158.5 kHz) の強い励起，伸縮モード (276.0 kHz) の弱い励起，伸縮モード (276.0 kHz) の強い励起

縮モード (276.0 kHz) の励起を示す．伸縮モードを励起するためには，重心モードの励起と比較して 300 倍の電圧を印加する必要があった（重心モードの 0.01 V に対して 3 V）．それより高次のモードの励起にはさらに大きな交流電圧が必要であり，文献 [212] の実験系では印加できる最大電圧の制約から，高次モードの励起は行えなかった．実験で用いた励起電界はイオン鎖方向に対してほぼ均一であるが，高次のモードを励起するためには大きな電界の勾配をイオン間に発生させる必要があるため，効率的な励起が難しい．

重心モードは均一の電界で励起されるため，電界の揺らぎに非常に敏感である．しかし，この揺らぎはイオン間距離と比べると非常に小さく問題にならない．一方，高次モードの励起には大きな勾配が必要となる．よって，不必要な高次モードの励起はあまり起こらない．これは量子計算に不利のように見えるが，実際の量子計算では，レーザと各イオンの相互作用に基づくサイドバンドのラマン遷移によって振動量子の振動が励起できる．

5.3.5　量子レジスタとしてのイオン

イオンの二つの電子状態 $|g\rangle, |e\rangle$ の一方を，または重ね合わせを利用すれば量子情報がイオンに蓄えられる．さらに，これら 2 状態には量子計算終了まで耐えうる十分に長い寿命を有することが望まれる．一つの可能性は，イオンの基底状態と擬安定な励起状態の一つを組み合わせること，そして場合によっては擬安定な二つの励起状態を利用することである．寿命は，単純な量子計算が十分実現できる秒のオーダをもつことが知られている（図 5.21(b) に示す $^{40}Ca^+$ の ^2D 準位がそのよい例である）．双極子との相互作用による電子状態の緩和より安定な基底状態の超微細構造を利用すれば，さらに長い寿命が実現できる．$^9Be^+, {}^{25}Mg^+$，$^{43}Ca^+$ などが利用可能で，図 5.21(c) にベリリウムの例を示す．超微細構造をもたないイオンでは，量子情報は基底状態のゼーマン分裂を利用して蓄えることもできる．通常，イオンは二つのゼーマン基底状態を有するため，この方法は後述の位相ゲートのような量子ビット演算につながる．N 個のイオンがトラップできればヒルベルト空間における $2N$ 次元が網羅された量子計算が発展する．

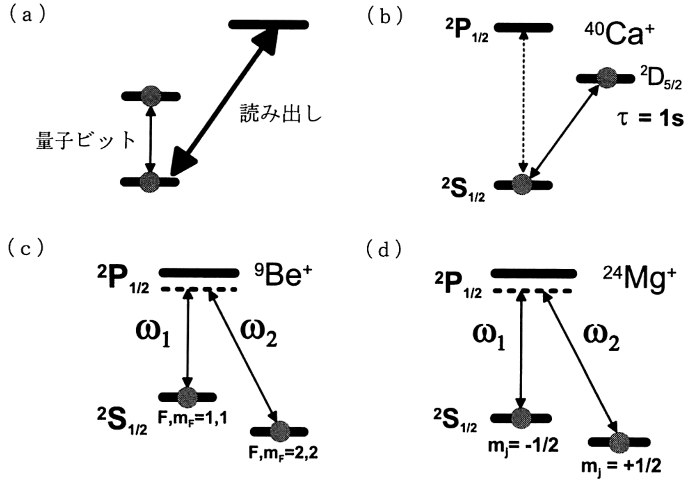


図 5.21 量子計算に利用される捕捉されたイオンのエネルギー準位図．(a) 効率的な読み出しのための遅い量子ビット内遷移と速い量子ビット外遷移を含む 3 準位系．(b) 基底状態と擬平衡状態を量子ビットに含む系．(c) 基底状態の超微細構造を利用する量子ビット．(d) ゼーマン準位を利用する量子ビット

5.3.6 単一量子ビットの準備と操作

量子計算の実施に先立ち，入力されたデータは量子レジスタに蓄える必要がある．このプロセスは，N 個のイオンそれぞれを特定の電子状態に励起することに対応し，イオンの内部状態のレーザによる操作で通常は得られる．イオン間の距離は 10 μm のオーダで，レーザの焦点をこのイオン間隔以下に絞ることで複数イオンの同時励起を回避できる．一つのレーザ光線を音響光学または電気光学的効果を利用して曲げ，鎖上の各イオンに順番に照射するのがよいであろう．本手法はインスブルックのグループによって実演された [213].

量子ビットの入力状態の準備は 2 段階で行われる．最初は初期化で，光ポンプ法などによって，基底である $|g\rangle$ または $|e\rangle$ のどちらかの状態にすべて量子ビットが設定される．このよく定義された初期状態に，2 準位の共振周波数を有するレーザパルスを照射し，時間に依存するラビ振動を誘発することによって，量子ビットの任意の重ね合わせ状態 $\alpha|g\rangle + \beta|e\rangle$ を準備する．π パ

ルスを照射すれば，量子ビットは直交した状態に回転され，さらに短いパルスを照射すれば重ね合わせの状態が準備される．ラビ振動は，位相情報を保ちながらの量子レジスタの操作，すなわち量子計算に必要な条件によらない単一量子ビットの回転にも利用される．

どのようにラビ振動を利用するかは実際に利用する構造によって変化する．量子状態が光学周波数によって分離されていれば，1光子遷移が利用される．超微細構造や，電子状態のゼーマン分裂を利用する場合は，二つのラマン光子が利用され，イオンの励起状態近傍に形成される擬準位を利用して量子ビット状態の相関が得られる．

5.3.7　量子データバスとしての振動モード

これまでは個々の量子ビットを独立して操作することを記述した．しかし，現実的な計算（論理演算）では，量子ビット間の強い相関が必要であり，イオン鎖における各イオンの状態は，他のイオンの状態によって変化することになる．イオン鎖における最も強いイオン間相互作用がクーロン斥力であり，平衡状態においては外的なイオン捕捉ポテンシャルとバランスを取りあっている．5.3.4項で述べたとおり，イオンは平衡位置を中心とした振動を行い，イオン同士は強い相関をもっている．異なる位置のイオン同士を相関させるという観点から特に興味深いのが，線形トラップにおける重心モードである．重心モードではすべてのイオンが位相を保って振動するため，鎖上の遠くに離れた特定のイオン間における量子情報の移動に利用できる．

計算の始めには，重心振動モードを量子力学的な基底状態に冷却する必要がある．そのためには5.3.3項で記述したサイドバンド冷却といった技術が利用される．その後，鎖状の任意のイオンの量子情報が次のプロセスによって移動される．まず1個のイオンに選択的にレーザ光線を照射し，πパルスをイオン共鳴より低エネルギーのサイドバンドに当てることにより，イオンの内部エネルギーを鎖の外部（振動）状態に移し変える（図5.22(a)参照）．その結果，重心振動モードの基底状態と第1励起状態は重ね合わせ状態となり，それはもともとのイオン内部状態における重ね合わせ状態に対応している．重心モードの振動は相関的であるため，鎖上のすべてのイオンが同様の振動運動を始め，結果として同じ量子情報に接することができる．よって，次節で述べるとおり，制御イオンの量子状態に依存して標的イオンの量子状態

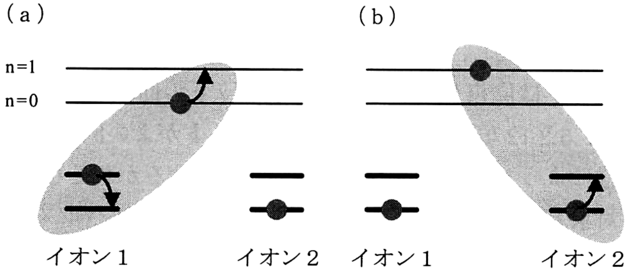


図 5.22 量子データバスとしてのイオンの振動モード. (a) 最初のレーザパルスでイオン 1 は重心モードへ移行され, (b) イオン 2 の状態は重心状態によって条件付きで操作される

を操作するという量子ゲートの任務は, 重心運動の状態に依存して標的イオンの量子状態を決定するという問題にすりかえられる (図 5.22(b) 参照). すなわち, イオン振動は鎖上の量子レジスタをつなぐ量子バスのように振舞う. 2 個めのイオンに対する演算が終了次第, これまでの逆のステップを通じて振動モードを基底状態に戻し, 同時に 1 個めのイオンを初期状態に戻す必要がある.

5.3.8 イオントラップ量子計算における 2 ビットゲート

Cirac と Zoller によるイオントラップ量子コンピュータ提案の本質的な功績は, イオンの内部状態を入力量子ビットとした上で, 振動の重心モードを利用した 2 量子ゲートの実施方法を見いだした点にある. これから, 振動モードを制御ビットとして標的イオンの状態を制御する量子ゲートについて述べる.

最も単純なゲートは, たった 1 種類の基底の組み合わせのみが出力を変化させる場合である. 位相ゲートと呼ばれる演算の例では, 二つの入力量子ビットの両方が上の状態のときのみに系の波動関数の位相を π だけ変化させ (符号を反転をさせ) 出力するが, それ以外の入力に対しては何も行わない. 波動関数の符号を反転させるためには, 2π パルスをイオンに照射すればよい. 条件付き演算を実現するためには, ねらいとするイオンの内部状態の遷移とのみ相互作用をもつパルスを照射する必要がある. そのためには他の遷移からはっきりとエネルギー的に区別されたエネルギー準位の差が必要で, たとえばゼーマン準位や異なる電子準位が利用される. 振動状態に対する条件づけは, たとえば, 重心モードの高エネルギー側のサイドバンドに対応する光

を照射することで，少なくとも一つの振動量子がある場合にのみ遷移を誘発するようにする．ただし，この方法では2個以上の振動量子は励起できない．

その他のゲートは位相ゲートと単一量子ビットの回転を組み合わせることで可能となる．5.2.12項で示した制御NOTゲートがよい例で，ここでは制御ビットの状態によって標的ビットの状態を回転させるかさせないかを決める．たとえば，対象とする2準位系の共鳴条件を満たす $\pi/2$ パルスを位相ゲートの前後に当てることで，計算に用いる基底を $|g\rangle \pm |e\rangle$ に一時的に設定できる．振動モードを制御ビットとした制御NOTゲート動作は実験によりすでに示された[211]．

イオンによっては，ゼーマン分裂や超微細構造といったエネルギー的に他から差別された遷移がなく，上述の位相ゲートと単一量子ビット回転を段階的に行いづらい場合がある．そのときは，イオンの内部自由度と外部自由度の間の相互作用が励起された振動量子の数に非線形的に依存する性質を利用して，制御NOTを直接実施したほうがよい[233]．共鳴条件を満たすパルスは，その系が振動の基底状態にある場合は 2π パルス，その系が1個でも振動量子を有し振動の励起状態にある場合は π パルスとしてはたらく．よって，後者の場合でのみイオン状態は回転される．

5.3.9　量子ビットの読み出し

量子計算が終了した時点で，量子ビットレジスタ状態の測定，すなわち計算結果の読み出しを行う必要がある．これはイオンの量子状態を選択した基底に射影する操作に相当する．

イオントラップ量子コンピュータの特徴は，単一イオンの量子飛び越え（ジャンプ）を検出することにより[234]，読み出しにおいてほぼ100%の検出効率を得られることにある（5.2.8項）．量子ジャンプ後の各イオンには，その量子ビットの状態のみと相関をもつ周波数のレーザ光が照射され，それによって励起された遷移が放射再結合する際に生じる発光が読み出しとして検知される（図5.23）．散乱光の存在は，相関状態が占有され，直交する基底状態が占有されていないことを同時に示唆する．重ね合わせ状態の検知は，量子ビットを測定前に回転させることによって行われる．

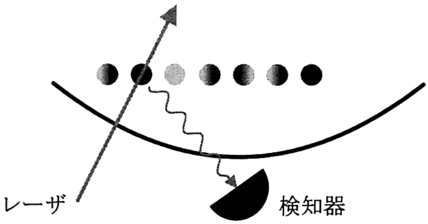


図 5.23 イオンの量子ビット状態の測定．読み出しのための遷移（図 5.23(a) 参照）に正確に波長が設定されたレーザ光線によって各イオンが選択的にアクセスされ，発光が検知される

5.3.10 結論

本節ではイオントラップの基礎的な動作原理と量子計算への応用について述べた．現時点では，線形イオントラップ中に捕捉されたイオン鎖が，量子計算の基本原理を示すための最もすぐれた候補であろう．イオントラップの本質的な長所は，イオン内部状態の長い位相緩和時間と，レーザを用いて量子ビット状態を準備し，制御し，読み出せることである．役に立つ量子アルゴリズムの実現には集積化（多量子ビット化）が不可欠であるが，これまでに提案されたさまざまな量子計算法の提案と比較しても，イオントラップが最も高い可能性を有することが，少なくとも理論上は予測される．

しかし，現実のイオン量子コンピュータでは，実験上のさまざまな問題が計算能力を制限する．電界の揺らぎや，真空槽内におけるイオンの残留ガスとの衝突は位相緩和速度を高め，最悪の場合はイオンの内部状態の発光寿命より速くなるかもしれない．さらに現実的な問題がイオン鎖の位相緩和である．1 個のイオンを振動の基底状態に保ちたい場合でも，その寿命は $^{198}Hg^+$ で 0.15 秒 [214]，$^{9}Be^+$ で 1 ms[211] 程度で，望まずして振動が励起されてしまう（$^{40}Ca^+$ に対する実験結果は Ref. [215] に示された）．位相緩和は，量子計算が実施できる演算ステップ数を制限してしまう．このような問題を克服すべく，最近では伸縮モードを利用した量子データバスに関する実験も進められている [212, 216]．

量子計算の性能に制約を与える要因として，演算中に生じる実験上の誤差についても考えなければいけない．利用されるレーザのパルス時間や間隔，周波数設定や強度，イオンの位置などを実験では完璧にすることはできない．

しかし，実験上の誤差はエラー修正と呼ばれるソフトウェア面のコードやプロトコルの発展によって解決される可能性がある．

トラップのサイズと冷却に用いるレーザパワーさえ任意に調整できれば，イオントラップに捕捉できるイオンの数に理論的な上限はない．しかし，これまでに実現された実験の最高記録は，2 個のイオンを捕捉して基底状態まで冷却した程度である [216]．この数は数年以内に数十個に増えるであろうが，Shor の因数分解アルゴリズムを実用化するためには，数千の量子ビットと数十億のレーザパルスが必要となる．現時点ではそのような実験はほぼ不可能に見える．しかしイオントラップは，小規模ではあるが量子計算の基礎概念やエラー修正方法のテストに向けて最も適した系であろう．すなわち，エンタングルした量子状態を作り出し，操作し，読み出すための理想的な実験環境をイオントラップが提供してくれる．

5.4　核磁気共鳴実験

(*J.A Jones*)

5.4.1　はじめに

核磁気共鳴 (NMR: Nuclear Magnetic Resonance) は磁場中における原子核のゼーマン分裂した準位間の遷移を調べる手法である．このように一言で済ませると重みに欠けるが，実際には分子科学における最も重要な分光手法といっても過言ではない [235,236]．その理由は，核磁気共鳴の周波数が原子核がおかれた化学的な環境によって正確に変化するため，核磁気共鳴のスペクトルを注意深く解析することによって対象とする分子の構造が決定できるからである．

NMR は量子コンピュータを実現する可能性を有する技術であると長いこと考えられてきた．その魅力は時には過大評価され，核スピンは量子ビットとして最もふさわしく，NMR では比較的容易に量子論理ゲートが構成できると主張されたが，NMR 量子コンピュータではよく定義された初期状態を得ることが困難であり，初期化なしでは興味深い計算が実行できないという欠点があった．ところが，最近になってこの問題が二つの独立した手法により

解決され，大きな進展が得られた [237]-[239].

分子科学における重要性のおかげで，NMR 分光器に関する技術の進歩はすばらしい．多額の資金が各部品の品質向上に投入され，市販の分光器でさえ理論限界に近い性能を発揮している．最新の NMR 分光器は複雑な構造を有するにもかかわらず扱いが容易で，最も神経質な理論家でさえ自らの操作で簡単な実験が行えるまでに進歩している．

5.4.2 NMR ハミルトニアン

NMR ハミルトニアンは最悪の場合には複雑になるが [236, 240, 241]，多くの実験では単純化され複雑な部分は無視できる．まず，単純な例としてスピン 1/2 を有する原子核（たとえば ^{1}H, ^{13}C, ^{15}N, ^{19}F, ^{31}P）の場合を考える．これらの核では大きな核スピンを有する原子核で考慮すべき多くの相互作用が無視できるからである．また，スピン 1/2 を有する原子核が 2 準位系であるという点でも量子ビットの候補としてふさわしく，NMR 量子コンピュータの実現にむけて最も重要な原子核といえる．次に NMR 試料が液体（通常，純粋な液体か溶液）であることを仮定する．液体中の分子の急速な運動のおかげで，異方的相互作用が等方的に平均化され，多くの場合はゼロになるため，NMR ハミルトニアンは大幅に簡略化される．溶液中のスピン 1/2 原子核から得られる NMR ピークの幅は非常に小さく，そのような測定は高分解能 NMR と呼ばれている [242].

高分解能 NMR では二つの相互作用が特に重要となる．1 番めはゼーマン相互作用である．z 軸方向に磁場 B_z が存在する場合，二つのスピン状態の縮退 $(I_z = \pm\frac{1}{2}\hbar)$ はゼーマン相互作用によってとかれる．

$$H = -\gamma I_z B_z \tag{5.19}$$

ここで γ（磁気回転比）は核種特有の定数である．典型的な NMR 磁石中のゼーマン分裂は ^{1}H に対して 500MHz 程度であるため，NMR 実験にはラジオ (RF) 波が用いられる．

分子間の平均距離が数Å の溶液では，利用する RF 波の波長が分子間の平均距離より長く，また各分子が非常に激しく運動しているため，単独の分子のみを取り出す局所的プローブ技術を追求することは非現実的である．よって，溶液 NMR ではすべての分子からの協調的信号が検知される．このこと

は，NMR 実験における量子計算が単独のスピン系で行われるのではなく，多数の同様の分子の統計的集合体によって実施されることを意味する．この状況においては，磁場が分子内の原子核を取り囲む異なった電子の環境によって遮蔽され，それぞれの原子核の磁気回転振動数がその独特の環境に合わせて変化する．よって，特定の分子内の異なる原子核では NMR 遷移周波数に違いが現れる．この性質を利用すれば，多数の同種の分子の集合体であっても，各分子内の特定の核を集合体として周波数的に区別して測定・操作することが可能となる．

高分解能 NMR で 2 番めに重要な相互作用がスカラー結合（J 結合）である．これは，分子の運動によって平均化され無視できる単純な双極子–双極子結合とは異なり，フェルミ接触相互作用に関連した結合である．二つの原子核 I と S の相互作用が，それらの NMR 周波数の違いより小さい場合（弱結合），結合ハミルトニアンは単純化される．

$$H = J_{IS} I_z S_z \tag{5.20}$$

ここで J_{IS} は分子構造の詳細に依存するスピン–スピン結合定数である．この結合は，NMR スペクトルにおける同種原子核ピークの J_{IS} 程度の分裂として直接観測できる．

簡単な例： 図 5.24 に重水素で置換したシトシン分子を示す．シトシンは DNA の情報をつかさどる四つの基底のうちの一つであり，最近では NMR 量子コンピュータの実現に利用された [243]．そのためには，分子を D_2O に溶かし込むことにより，分子中の三つの水素が重水素で置換された．図 5.25 に，500MHz 分光器で得られたこの分子中の ^1H スペクトルを示す．2 個の ^1H 原子核に起因する主ピークが左右に分裂し，さらにそれぞれのピークが分裂した 2 重項（ダブレット）となっている．主ピークの分裂は 763Hz 程度で，500MHz 付近に観測される．各 2 重項のわずかな分裂 (7.2 Hz) はスピン–スピン結合の結果である．

5.4.3　NMR 量子コンピュータの構築

いくつかの量子コンピューティングのモデルのうち，最も一般的なのが量子演算回路を用いる手法である．そのような量子コンピュータは四つの要素

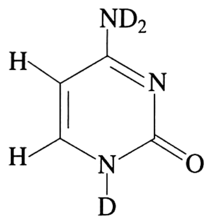


図 **5.24** 重水 D_2O に溶かし込むことによって一部が重水素化されたシトシンの構造．窒素に結合した 3 個の水素が重水素によって置換され，2 個の ^1H 原子核が隔離されたスピン系として利用できる．その他の原子核は無視してよい



図 **5.25** 一部が重水素化されたシトシン中の ^1H の NMR スペクトル．左右の 2 重項ピークのそれぞれがシトシン中の 2 個の ^1H からの信号に対応する

によって構成される．一つめは量子ビット で，スピン 1/2 の原子核の 2 準位系が利用される．核磁気共鳴においては比較的容易な部分である．残りの要素の実現はもう少し複雑である．

量子ゲート：量子演算回路は量子ビットを量子ゲートにより結合することから構築される．ゲートの構築方法には何通りもあるが，いかなるゲートも，単一量子ビットゲートと 2 量子ビットゲートの適切な組み合わせで実現できることが知られている [244]．単一量子ビットゲートはヒルベルト空間における単一スピンの回転に相当し，これは RF 波の適切な照射により達成できる．制御 NOT に代表される 2 量子ビットゲートの構築は，2 量子ビット間の相互作用制御による条件付きスピン運動変換を伴うため，さらに複雑である．NMR ではスカラー結合を利用することになる．スカラー結合は，単独では 2 量子

ビット間における制御ゲートの構築には適さないが，その組み合わせを行うことによって制御ゲートが実現される [245]．たとえば，制御 NOT ゲートでは，一対の単一量子ビット・アダマールゲート間での位相シフトを制御するゲート操作に基づき，標的量子ビットの状態を操作することを行う．位相シフトを制御するゲート（いわゆる制御ゲート）では $|11\rangle \to -|11\rangle$ 変換を行うと同時に，もう一方の基底状態を変化させないという操作を行う．位相シフト制御ゲートは，スカラー結合状態におけるスピン状態の時間発展（すなわち 2 量子ビットの回転）を単一量子ビットの位相シフトゲートと適切に組み合わせることによって達成される [245]．

消去（クリア）演算子： 量子演算ゲートは量子ビットをある状態から他の状態へ遷移させる操作である．しかしこの操作は，完全に定義された入力状態（初期状態）からスタートしなければ意味をなさない．現実には，任意の量子ビットをある特定の状態に遷移させる方法さえ確立できれば，そこからの単一量子ビットゲートの組み合わせで任意の入力状態が用意できる．初期状態としてふさわしい状態はクリア（すべてゼロに初期化）演算で得られる $|0\rangle$ であることは明らかであろう．

クリアは基底エネルギー状態に量子ビットを設定することに相当するので，原理的には低温化によって容易に達成できる．しかし，NMR では低温化プロセスに頼るのは残念ながら現実的ではない．ゼーマン分裂によって得られる 2 準位のエネルギー差が，実験室で得られる低温（ボルツマンエネルギー）より小さいからである．室温におけるエネルギーギャップは kT と比較してあまりにも小さく，上と下の状態の占有確率の差は割合にして 1 万分の 1 程度と，きわめて小さい．すべての状態に平均的に分布している場合では，スピン状態の遷移も平均化され打ち消しあい，結果として NMR 信号は得られない．一方，平均からずれた状態（上述の例では 1 万分の 1 程度の非熱平衡分布）からは NMR 信号が検出される．

隔離された単一の原子核を有する分子（1 個の量子ビットを含むコンピュータ）では，実効的な $|0\rangle$ 状態を得るのは容易である．熱力学的平衡状態においては，高エネルギー状態 $|1\rangle$ と比較してごくわずかに低エネルギー状態 $|0\rangle$ の占有確率が増加するため，初期化されたとみなすことができる．しかし，この単純な考え方は多量子ビットを有する状態には拡張できない．多数の量子

ビットを対象とすると，集合体としての占有確率の差は複雑化し，初期化とみなせる状態をとらない．結果として，クリア（初期化）ができないという現実が，NMR 量子コンピュータの発展を何年間も妨げた．

ところが，この問題を解決する二つの方法が 1996 年後半に発見された [237, 238]．ここでは複雑な NMR のパルス系列を用いてさまざまなスピン状態の占有確率を操作し，結果として初期化状態とみなせる状態を用意する．一方，Chuang と Gershenfeld はスピン状態を異なる部分集合に分離することを提案した [239, 246]．部分集合のなかには熱平衡状態における初期化と同様の分布を有するものが存在し，それを選び出すことにより初期化状態を得ることに成功した．この方法は理論的には洗練されているが，実際に用いるには複雑で，広く使われていない．さらに最近では，テンポラル平均 (temporal averaging) [247] などの手法も提案されているが，Cory らの手法の延長という観点からここでは言及しない．さまざまな初期化法の詳細なる比較は Havel らのグループが行った [248]．

出力： 計算の終わりに最終結果を読み出す機構が必要となる．固有状態の計算結果である 1 個または複数の量子ビットの状態を読み出すステップであるが，NMR 量子コンピュータでは，各量子ビットにおける $|0\rangle$ と $|1\rangle$ 状態の占有確率の違いを知ることが読み出しに相当する．占有状態の差を直接測定することは現実的ではなく，実際には 90° パルスを利用して $|0\rangle$ と $|1\rangle$ 状態のコヒーレントな重ね合わせ状態をつくる．その状態は磁場中で振動するため，占有確率の相対値は，振動の振幅と位相を観測することによって得られる．ここでは位相の絶対値は意味をもたないが，基準信号との相対的位相差を測定することにより目的を達成する．

いくつかの量子アルゴリズムは複数の量子ビットを占有する結果を導くが，その場合は 2 種類の読み出し方法が提案されている．一つは，複数の量子ビットのうち 1 個のみのスピンを励起し，そのスピン信号の分裂を正確に測定することによって他量子ビットの状態を決定する．もう一つは，すべてのスピンを同時に励起し観測する．この場合，各スピンの状態は NMR 信号の位相から得ることができる．

他の方式と比較して，NMR 量子コンピュータでは重ね合わせ状態が直接観測できるため，結果を固有状態として保持しなくてよいという利点がある．

重ね合わせ状態が観測できるのは NMR 特有のアンサンブル平均という読み出し方法による．単一スピン系の測定では重ね合わせ状態が崩壊するが，弱い測定であるアンサンブル平均ではそのようなことは起こらない．よって，二つの相互作用を有する状態の観測を連続的かつ同時に行うことが可能となる．このような長所は今後の実験でも威力を発揮するであろう．

5.4.4　Deutsch の問題

ここまでの概念的記述は，Deutsch の問題を解くための NMR 量子コンピュータの構築で具体性をもつことになる [138, 249]．この問題は 4.2.4 項で詳しく述べられているため，ここでは簡単なまとめだけを述べる．次の 2 進関数を考えよう．

$$f(x) : B \mapsto B \tag{5.21}$$

また，関連する演算子 U_f を以下のとおり定義する．

$$|x\rangle|y\rangle \longrightarrow^{U_f} |x\rangle|y \oplus f(x)\rangle \tag{5.22}$$

これらから，図 5.26(a) に示す $f(0)$ と $f(1)$ を決定する量子回路を構築することが可能となる．Deutsch の問題とは，たった 1 回の演算 U_f のみで $f(0) \oplus f(1)$ を決定することを目的とする．これは古典コンピュータでは不可能であるが，量子コンピュータでは図 5.26(b) に示す回路で可能となる．

この回路は，シトシン分子の一部の水素が重水素によって置換されたわれわれの NMR 量子コンピュータによって実現された [243].（同様の結果は Chuang らのクロロホルム量子コンピュータでも得られている [250].）われわれの NMR 量子コンピュータでは各ダブレット（2 重ピーク）が単一量子ビットからの信号に対応している．量子ビットの値は信号の位相（正の場合は $|0\rangle$ 状態で，負の場合が $|1\rangle$ 状態）から決定できる．

すでに述べたとおり，NMR 信号の位相の絶対値はさまざまな実験条件に依存するため，大きな意味をもたない．しかし，相対的な位相は重要であるため，基準となる信号の位相を正しい絶対値に調整することにより，その基準位相からの相対的位相を正確に測定することで，対象とする信号の位相の絶対値が決定できるようになる．二つの異なる実験の位相比較も，実験条件を完全にそろえることによって可能となる．よって，一つに実験によって得

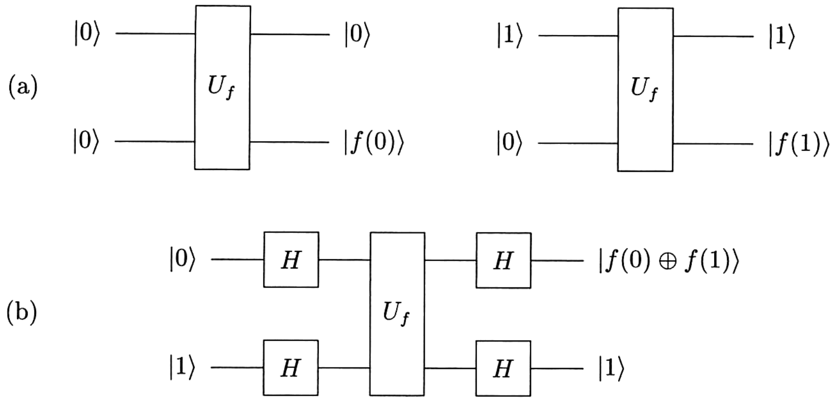


図 5.26　(a) 2 進関数における $f(0)$ か $f(1)$ を決定するための量子回路．(b) $f(0) \oplus f(1)$ を 1 回の演算子 U_f で決定するための量子回路（Deutsch の問題）．H は単一量子ビットに対するアダマールゲート

られた基準位相をもとに，二つめの実験の信号の位相を決定することができる．以下に記述する実験では，そのような手法が用いられた．

図 5.27 に古典的アルゴリズムによって実験的に決定された $f(0)$ を示す．このアルゴリズムでは左側の列の第 1 量子ビットが入力に対応し，右側の列の出力が第 2 量子ビットに対応する．表 5.1 に四つの 2 進関数に対する結果を示す．予想のとおり，左側の信号は，$f(0) = 0$（すなわち f_{00} と f_{01}）の場合に常に正であり，$f(0) = 1$（すなわち f_{10} と f_{11}）の場合に負となる．これらのスペクトルの絶対的位相は不明であったが，この問題はスペクトル (a) を基準として位相修正を行い，同様の位相修正を他のすべてのスペクトルに行うことにより解決された．

また，図の信号では主ピークのダブレット分裂までは見えて（分解されて）いないが，本量子コンピュータの枠組みのなかでは，すべての多重ピークが同じ符号を有するため問題とはならない．理想的には符号は単純に正か負であるが，実際に得られる信号はもう少し複雑となる．同様に，すべてのピークが同じ強度を有するべきであるが，実験結果はそうではない．これらのエラーは量子ゲート操作の不完全性に起因するが，少なくとも系統的である．よって，これらの問題はパルス系列等の改善に基づくゲート操作精度の向上



(a) f_{00}　(b) f_{01}　(c) f_{10}　(d) f_{11}

図 5.27　NMR 量子コンピュータによる $f(0)$ を決定するための実験結果. 組み合わせとして可能な四つの 2 進関数 f の結果を示した

表 5.1　1 ビットを回転させるための 2 進関数で，組み合わせとして可能な四つの例

x	$f_{00}(x)$	$f_{01}(x)$	$f_{10}(x)$	$f_{11}(x)$
0	0	0	1	1
1	0	1	0	1

によって解決できる.

同様のアルゴリズムを利用して $f(1)$ を決定することもできる．ここで必要となるのが入力値の工夫であり，その例を図 5.28 に示す. ここでは，左側の信号は常に負だが，右側の信号は負または正の値をとる．予想どおり，この信号は $f(1) = 0$（すなわち f_{00} と f_{10}）の場合は正で，$f(1) = 1$（すなわち f_{01} と f_{11}）の場合は負となる．ここでも図 5.27 と同様の位相補正を行った.

結果として，この量子コンピュータでは Deutsch の問題（$f(0) \oplus f(1)$ の決定) を解くことが可能となり，その結果を図 5.29 に示す. 量子コンピュータでは可能性がある二つの入力状態の重ね合わせを利用するため，この例では入力ビットは存在しない．そして結果は左側の信号の位相として表される．二つめの量子ビットは，単純に演算を行うビットであり，計算開始前と終了後は $|1\rangle$ 状態にある．予想されたとおり，右側の信号は常に負であり，左側は f_{00} と f_{11} （すなわち $f(0) \oplus f(1) = 0$）の場合は正で，f_{01} と f_{10} （すなわち $f(0) \oplus f(1) = 1$）の場合は負となる.

5.4.5　量子探索とその他のアルゴリズム

擬純粋初期状態が実効的に得られることが可能となった時点から，NMR 量子コンピュータは急速に発展した．2 個の量子ビットを有するコンピュータによって，2 量子ビットを探索場とする Grover の量子探索アルゴリズムが実



(a) f_{00} (b) f_{01} (c) f_{10} (d) f_{11}

図 5.28 NMR 量子コンピュータによる $f(1)$ を決定するための実験結果．組み合わせとして可能な四つの 2 進関数 f の結果を示した



(a) f_{00} (b) f_{01} (c) f_{10} (d) f_{11}

図 5.29 NMR 量子コンピュータによる $f(0) \oplus f(1)$（Deutsch の問題）を決定するための実験結果．組み合わせとして可能な四つの 2 進関数 f の結果を示した



(a) $|00\rangle$ (b) $|01\rangle$ (c) $|10\rangle$ (d) $|11\rangle$

図 5.30 NMR 量子コンピュータによる 2 量子ビットを探索対象とした場合の Grover の量子探索の実験結果．組み合わせとして可能な四つの解に対する結果を示した

現された [251]-[253]．ここでは四つの可能性を有する探索対象の中から一つの正解が，たった一度の探索ステップで見つけられた．アルゴリズムは量子コンピュータが $|00\rangle$ の状態から開始され，1 回のステップで探索対象である $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ のいずれかが得られる．図 5.30 にシトシン量子コンピュータを利用して得られた 2 量子ビット量子探索の結果を示す [252]．正確にはこの結果はパルス系列を工夫することにより得られた最近の結果であり [254]，初期の発表 [252] より信号が向上されていることに注意されたい．

NMR 量子コンピュータは，たった一つの探索対象を有する場合の Grover の量子探索の単純形に対して威力を発揮する．しかし，より一般的な探索対象（正解）が複数になる場合では困難が生じる．対象が複数となると一般的な量子コンピュータは複数正解の中から一つを解として提示するが，NMR 量子コンピュータでは複数正解の一種のアンサンブル平均を解として提示し，その状態から意味のある情報を得ることは現時点ではほぼ不可能に近い．近似的量子カウンティングという手法によって回避する提案もなされている [254] が，今後の発展が期待される．

3 量子ビット系に関する研究も進んでおり，興味深い量子現象である GHZ 状態 [255, 256]，単純なエラー修正プロトコル [257, 258]，テレポーテーション [259] が調べられ，Deutsch-Jozsa アルゴリズムの実行 [260] に成功した．Deutsch-Jozsa アルゴリズムに関しては 5 キュービットに対する成功も得られている [261]．

5.4.6　将来の展望

現在の手法を基盤とすると，大規模 NMR 量子コンピュータの実現にはいくつかの大きな問題を乗り越える必要がある．一般的に最も懸念される問題が，量子ビット数の増加とともに信号強度が指数関数的に減少することで，それと並行してデコヒーレンスに関する懸念も議論されている．実際の実験では，信号強度とデコヒーレンスが問題となるのはずっと先のことであり，その前にさまざまな異なる問題を乗り越える必要がある．しかし，信号強度の減少とデコヒーレンスは原理的な問題でもあるので，まずそれらに関して議論しよう．

指数関数的信号強度の減少： 量子ビット数の増加に伴う指数関数的信号強度の減少は，擬純粋状態を熱平衡状態の行列要素から抽出する必要性から生じる．1 個の量子ビットの追加は，1 個のスピンの追加を意味するため，系全体として得られるスピン状態数が倍になる．擬純粋状態の抽出では系の中の任意の単一スピン遷移を利用するが，この遷移に関する状態が 1 個のスピンの追加によって二つに分裂するため，結果として信号強度が減少する [262]．この問題は NMR に特有のものではなく，$\Delta E \ll kT$ という高温を利用するすべてのアンサンブル平均量子計算において生じる問題である．

指数関数的信号強度の減少が問題となる可能性はあるが，実際に懸念されているほど深刻とは考えていない．NMR 信号は高い S/N 比（図 5.25 の例では 800）で得られるため，指数関数的信号の減少は量子ビット数が 10 を超えない限り深刻な問題とならない．また，さまざまな手法によって NMR における S/N 比を向上させることもできるであろう．信号の積算や試料サイズを大きくすることが単純な対応策であるが，光ポンピングによるスピン偏極率増大も考えられている [263].

Schulman と Vazirani は忠実度の低い量子ビットの集合系を純粋化する計算手法を提案した [246]．この手法は熱平衡状態のスピン分布に対しては適用できないが，光ポンピング等のスピン偏極を増大させる手法と併用することによって有用となるかもしれない．

デコヒーレンス： 他のすべての量子コンピュータと同様に，NMR 量子コンピュータでもデコヒーレンスを抑えることが重要となる．デコヒーレンスとは，コヒーレントな重ね合わせ状態がランダム過程によってコヒーレントではない状態に移行することを指す．すべての重ね合わせ量子状態は特有の位相緩和時間を有するため，緩和時間よりあまり長くない時間内に量子計算を完了する必要がある（ただし，エラー修正法によってこの計算時間の延長は可能である）．NMR 量子計算では，スピン－スピン緩和時間 T_2 が重要となる．ただし，一般的に T_2 とは単一スピンの緩和を指すが，ここでは複数のスピン系における緩和を指し，単一スピンの T_2 とは異なる場合がある．しかし，単一スピンの T_2 と集合体の T_2 の間にはある程度の相関があると期待されるため，T_2 とまとめて考えることが多い．現在調べられている小さい分子の溶液に基づく NMR 量子コンピュータでは，数秒の緩和時間が得られている．

量子コンピュータで重要となるのは緩和時間の絶対値ではなく，緩和時間と 1 回の量子ゲートの実行に必要な時間の比である．制御 NOT のような単純な 2 量子ビットゲートを実行するのに必要な時間はスカラースピン・スピン結合の逆数（約 5～150 ms）であるため，数秒の緩和時間とあわせると数十から数百のゲート操作が可能になると考えられる．T_2 が飛躍的に長い系も知られているが，量子ゲートを実現するために十分なスピン－スピン相互作用が得られないため，それらを利用して現在の NMR 量子コンピュータのコンセプトを実現することはできない．

その他の問題： 上述の二つの懸念以上に重要な問題が，スピン数の増加とともに任意のスピンへの選択的アクセスが困難になり，ゲート操作が複雑化することである．

スピン数の増加とともに任意のスピンへの選択的アクセスが困難になることは明らかであろう．一般的な量子コンピュータでは，各量子ビットが位置的に区別されるが，その方法は NMR 量子コンピュータでは適用できず，NMR 遷移周波数の違いによって区別される．しかし，区別するための周波数領域が比較的狭く（典型的には数千 Hz），NMR 周波数が近い複数のスピンのなかから単独のスピンのみを選択的に励起することが難しい [265]．これが実験的に得られるスペクトルを歪める大きな要因となっている（図 5.27〜5.30）．スピン数の増加とともにすべてのスピンが十分な周波数差をもつことが難しくなり，よって選択性が悪くなる．

この理由から，これまでに発表された多くの実験では，クロロフォルム中の ^{1}H-^{13}C のように，異なる核スピンを含む分子が調べられた．この場合には二つのスピンの共鳴周波数は数百 MHz も異なるため，各スピンの選択的励起が非常に容易となる．この手法によって 2〜3 個のスピン系の実験が進展したが，利用できる核の種類には限りがあり，NMR 分光器ではせいぜい 2〜3 種類の核しか同時に扱えないことからも，多数スピン系への延長は困難である．よって，3 個以上のスピンを含むすべての NMR 量子コンピュータが選択的スピン励起の問題に直面する．

複数スピン系における量子演算ゲートの複雑化もあまり議論されていないが重要な問題である．理想的には 2 量子ビットコンピュータに対して開発された 2 量子ビットゲートの操作方法をほぼそのままの状態で 3〜4 量子ビットゲート操作に拡張できればよいが，NMR 量子コンピュータでは容易でない．スピン–スピン結合に代表されるゲート操作に関連する相互作用が背景ハミルトニアンに含まれるため，特定の励起がない状態においてもスピン系は時間発展する．量子演算ゲートの実現には，背景ハミルトニアンの構成要素の強度を変調することによって得られる実効的なハミルトニアンが利用される．しかし，量子ビット数の増加とともに，変調すべき相互作用の数が増えると同時に，不必要な相互作用を断ち切るための操作量も増加する [260]．N スピン系の背景ハミルトニアンには，最大で $\frac{1}{2}N(N+1)$ 個の単一および 2 スピン相互作用が存在するが，任意の 2 量子ビットゲートの実現にはそのうちのわ

ずか三つの相互作用のみが必要となる．当初はあまり心配されていなかったが [267]-[269]，これらの不必要な相互作用を断ち切ることは，10 量子ビット以上の NMR 量子コンピュータの構築に向けて最も難しい問題となりえる．

その他の手法： 上述のさまざまな問題を意識した一部の研究者は，同じ NMR を利用する場合でもまったく異なる量子コンピュータの構築方法を考えるようになった．そこで考え出される NMR 量子コンピュータは，これまでに述べた典型的な NMR 量子コンピュータとは大きく異なる．ただし，新しいアイデアで量子計算が実行された例はまだない．

多くの新しい提案に共通する点が，溶液でなく固体を利用することである．固体を用いることには NMR という視点から都合の良い点と悪い点がある．固体中の分子は溶液と比較して静的な状態にあり場所を移動しないため，原理的には単一分子を位置的に選択して励起することが可能となる．単一分子を直接的に選択するには RF 波の波長は長すぎるが，NMR イメージング技術 [270] を用いればスピンの位置的選択ができる．しかし，この手法によって原子レベルの位置分解能を得ることは難しい．その理由として，大きな磁場勾配を発生させることが困難であることと，NMR の検知限界を考慮した場合に単一スピンを検知することが難しいこと [270] があげられる．計算によると，分解能の限界は 1μm 程度であるため，単一スピンよりもスピンのクラスター集合体を利用する必要がある．

また，溶液では分子の異方的な相互作用は平均化され等方的に扱えたが，固体では異方的相互作用が NMR ハミルトニアンに含まれることになる．よって固体におけるスピン間相互作用では，スカラー結合よりはるかに強く直接的な双極子－双極子結合が支配的になるため演算ゲート速度が向上する．しかし，すべてのスピン同士が近接するすべてのスピンと結合するため，単一スピンの選択が困難になるうえ，デコヒーレンス時間が短くなるという短所がある．

最近の Kane による提案 [271] は，固体 NMR と既存のシリコンマイクロチップ技術を融合させ，上述の問題点に真っ向から向き合い，解決策を提示した点で高く評価できる．ここではシリコン中の隔離された ^{31}P 原子の核スピンを利用し，さらにゲート電圧を制御することから，単一スピン準位とその他のスピンとの結合を操作し，選択的励起を実現する．単一スピン検知に

は，核スピン状態によって変化する単一電子移動を用いる．この提案は現在のシリコンテクノロジーでは実現が難しいが，今後10年のテクノロジーの進歩によって多くの要素技術が実現される可能性は高い．

5.4.7　エンタングルメントと混合状態

最近，NMRは量子力学的手法ではないという指摘があった．このような指摘の根幹には，「量子力学的」という意味を，まったく古典力学が適用できない極端な場合に限る傾向があることにまず注意をしなければならない．対象とする準位間のエネルギー差より kT が大きい「高温領域」で実施されるNMR実験では，核スピン系を記述する密度行列はほぼ完全なる混合状態にあり，そのような状態は，異なる核スピン間のエンタングルメントがまったくない積の状態である [272]．NMR状態がエンタングルメントなしで記述できるのであれば，古典モードによっても記述できることになる（ここでの古典モードは単純ではない）．しかし，古典モデルで個々のNMR状態を記述できる一方，同様の古典モデルがNMR測定における個々の状態の時間発展を記述できるかどうかは明らかではない [273]．NMR量子コンピュータにおけるエンタングルメントと混合状態に関する議論はまだ続いており決着はついていない．

5.4.8　これからの10年

現時点において，NMRは量子コンピュータの構築に向けて最も効果的な技術であり，この状態はあと数年は続くと考えられる．いくつかの小規模なNMR量子コンピュータがすでに構築され，量子アルゴリズムが実行された．

これからの数年で3〜5量子ビットのNMR量子コンピュータの構築が定常化し，それ以上に大規模な系に関する基礎研究も進むであろう．しかし，現在の手法を大幅に改変しないかぎり10量子ビット以上のNMR系の構築は難しいと考える．長期的には，Kaneの提案のような固体NMRコンピュータが有用となる可能性が高い．

第6章

量子ネットワークと多粒子エンタングルメント

6.1　はじめに

前章では量子エンタングルメントの概念を導入した．この章では最先端のさまざまな話題を取り扱う．6.2 節では，空間的に離れた原子間での光子を媒介にしたエンタングルメントの生成について述べる．ここで述べるように，寿命が長く操作が簡単な原子やイオンと，広い適用性があり長距離でも信頼性の高い量子通信が可能な量子光学系を組み合わせて用いることで，量子ネットワークを構築することができる．

6.3 節では 3 粒子以上のエンタングルメント状態を扱う．このような状態は量子情報理論で大切であることはもちろんであるが，元々は Einstein-Podolsky-Rosen(EPR) の指摘した，局所実在論と量子力学の矛盾に関して研究が始まったものである．すなわち，Greenberger-Horne-Zeilinger(GHZ) が提唱した 3 粒子の GHZ エンタングルメント状態には，局所実在論と量子力学との矛盾がもっとも顕著な形で現れるのである．この節では 3 光子の GHZ 状態の生成方法について触れ，さらに 3 粒子以上のエンタングルメント状態が，古典的局所実在論の立場からはまったく理解不能な性質を示す理由を述べる．

最後の 6.4 節では，まず 3 粒子以上のエンタングルメントが非常に微妙な概念であることを示す．一般に 3 粒子以上のエンタングルメントを一意的に定義することはできない．次に 2 粒子間のエンタングルメントを定量化する尺度をいくつか紹介し，さらに関連した話題として，エンタングルメントの

抽出やエンタングルメントの相対エントロピー尺度などについて説明する．

6.2　量子ネットワークⅠ：離れた場所の間でエンタングルした粒子

(H.-J.Briegel, S.J. van Enk, J.I. Cirac, and P.Zoller)

6.2.1　原子と光子の媒介

量子ネットワークは，量子ビットが収容され局所操作が行われるノードとそれらを接続する量子通信路によって構成される．このネットワーク内での情報のやりとりは，量子通信路を量子ビットが通過することによって行われる．このようなネットワークを物理的に実現するには，たとえば図6.1のようにノードとして捕捉された原子かイオンの集団，量子通信路として光ファイバかそれに相当する経路を用いる．

原子やイオンは，量子ビットを特に長時間保持する目的に優れていて，最近提案されている捕捉された原子／イオン間の量子ゲートが各ノードでの局所操作の魅力的な手段を提供している [156,274,275]．一方で光子は，量子ビットの高速かつ長距離の伝送を実現する，最も信頼性の高い媒体である [276,277]．本節では，この原子と光子，つまりネットワークのノードと経路をどのように橋渡しするかについて述べる [278]．この方式により，離れた場所にある原子の集まり1と2の間で（原理的には）100%の効率で量子通信ができる．局所量子情報処理と量子通信を組み合わせることにより，エンタングルメント暗号 [279] や量子テレポーテーション [280]，さらにはもっと複雑な多者間通信や分散量子情報処理 [281,282] などの多くの斬新な応用への道が開かれる．

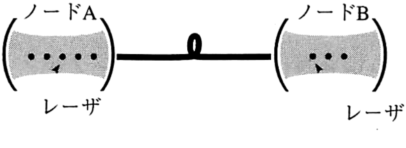


図6.1　量子ネットワークの素子．Q値の高い共振器に収容された原子は，量子情報の保持と局所的な量子情報処理を行う．この共振器がネットワークのノードつまり頂点に相当し，ネットワーク内の空間的に離れたノードとノードの間で量子情報を伝達するために光子が使われる

この方式の基本方針は，量子ネットワークのノードを構成しているQ値の高い光学的空洞共振器と原子の間の強い相互作用 [276] を利用するものである．まず始めにレーザ光を照射することによって1番めのノードにある原子の内部状態を光の共振器のモードに変換する．生成された光子は共振器から漏出し，伝達経路の上を波束の形で伝播して2番めのノードの共振器に入る．最後にその共振器での光の状態が原子の内部状態に変換される．一般にはエンタングルしている多くの量子ビットを伝達するには，量子ビットの個数分の原子をそれぞれのノードに配置しておく．そして，1番めのノード内のそれぞれの原子から2番めのノード内の対応する原子に状態を移す操作を順次行えばよい．この方式の優れている点は，原子と共振器の相互作用を制御することにより2番めのノードからの波束の反射を防ぐことができることである．それにより，通信中のデコヒーレンス（量子的な干渉性の消失）の主要原因となりうる通信路での損失をうまく抑え込むことができる．

6.2.2 量子状態伝送を表すモデル

二つのノード間の単純な量子伝送は，二つの原子1,2で構成されていて，それらはそれぞれの共振器のモードと強く結合している（図6.2参照）．

それぞれの原子の共振器との相互作用を記述するハミルトニアンは次のように表される $(\hbar = 1)$ [1].

$$\begin{aligned}\hat{H}_i = {} & \omega_c \hat{a}_i^\dagger \hat{a}_i + \omega_0 |r\rangle_{i\,i}\langle r| + g(|r\rangle_{i\,i}\langle g|\hat{a}_i + \text{h.c.}) \\ & + \frac{1}{2}\Omega_i(t)\left[e^{-\sqrt{-1}[\omega_L t + \phi_i(t)]}|r\rangle_{i\,i}\langle e| + \text{h.c.}\right] \qquad (i = 1, 2) \qquad (6.1)\end{aligned}$$

ここで $\hat{a}_i$ と $\hat{a}_i^\dagger$ はそれぞれ共振器のモード i（周波数 ω_c）の消滅演算子と生成演算子である．状態 $|g\rangle, |r\rangle, |e\rangle$ は励起周波数 ω_0 の3準位系を成し（図6.2

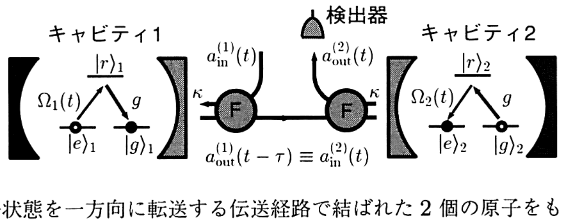


図 6.2 量子状態を一方向に転送する伝送経路で結ばれた2個の原子をもつ光学共振器

---

[1] 訳注：h.c. は Hamiltonian conjugate，つまり適当な項の共役作用素であり，式全体をエルミートに保つ．

参照），量子ビットは縮退した二つの基底状態 $|g\rangle, |e\rangle$ の重ね合わせとして記憶される．この状態 $|e\rangle$ と $|g\rangle$ はラマン遷移で結合している [274,275,283]．すなわち，周波数 ω_L のレーザが原子を時間依存するラビ周波数 $\Omega_i(t)$ と位相 $\phi_i(t)$ で $|e\rangle$ から $|r\rangle$ に励起したのち，その共振器でのモードの光子を放出しながら遷移 $|r\rangle \to |g\rangle$ が伴う（結合定数 g）．

ラマン過程での励起状態の光子の自然放出を抑えるために，レーザ周波数 ω_L は $|\Delta| \gg \Omega_1(t), \Omega_2(t), g, |\dot{\phi}_1(t)|, |\dot{\phi}_2(t)|$ （$\Delta = \omega_L - \omega_0$）を満たすように，原子の遷移周波数から大きく離調してある．

このような場合，断熱近似を用いて励起状態 $|r\rangle_i$ を無視することができる．共振器モードのレーザ周波数で回転する座標系での，二つの基底状態 $|e\rangle$ と $|g\rangle$ の新しいハミルトニアンは次のようになる．

$$\begin{aligned}\hat{H}_i = & -\delta \hat{a}_i^\dagger \hat{a}_i + \frac{g^2}{\Delta}\hat{a}_i^\dagger \hat{a}_i |g\rangle_{i\,i}\langle g| + \delta\omega_i(t)|e\rangle_{i\,i}\langle e| \\ & -\sqrt{-1}g_i(t)\left[e^{\sqrt{-1}\phi_i(t)}|e\rangle_{i\,i}\langle g|\hat{a}_i - \text{h.c.}\right] \quad (i = 1, 2) \end{aligned} \tag{6.2}$$

第1項はラマン離調 $\delta = \omega_L - \omega_c$ を含んだ項である．第2項と第3項はそれぞれ基底状態 $|g\rangle$ と $|e\rangle$ の共振器のモードとレーザ場による AC－シュタルクシフトであり，$\delta\omega_i(t) = \Omega_i(t)^2/(4\Delta)$ としてある．最後の第4項は，よく知られたジェインズ－カミングス相互作用で，有効結合定数を $g_i(t) = g\Omega_i(t)/(2\Delta)$ としてある．ここではラマン過程での自発放出による弱い影響はさしあたり無視してある．なお $|e\rangle, |g\rangle$ はそれぞれジェインズ－カミングスモデルの励起 (excited)，基底 (ground) に由来する．

時間依存のラビ周波数とレーザの位相を時間に依存させる理由は[2]，次のような理想的な量子伝送を実現するためである．

$$\begin{aligned} & (c_g|g\rangle_1 + c_e|e\rangle_1)|g\rangle_2 \otimes |0\rangle_1|0\rangle_2|\text{vac}\rangle \\ \to\ & |g\rangle_1(c_g|g\rangle_2 + c_e|e\rangle_2) \otimes |0\rangle_1|0\rangle_2|\text{vac}\rangle \end{aligned} \tag{6.3}$$

ここで c_g, c_e は複素数であって，一般にはこれらの変数は，「観測者」であるネットワーク内の他の原子の非規格化状態に置き換えられる．(6.3) において $|0\rangle_i$ と $|\text{vac}\rangle$ は，それぞれ共振器モードの真空状態と共振器の間の電磁波モー

[2] 共振器の透過率を変調するということも考えられるが，技術的により難しい．

ドの自由状態を表す．これらのモードを経由して光子を交換によって，量子ビットの伝送は行われる．

このような状況は量子軌跡 [284,285] の用語を用いて定式化すると都合がよい．2 番めの共振器が出力する場を光子検出器で継続的にモニターする仮想的な実験を考えてみよう（図 6.2 参照）．連続測定の下で，特定の測定結果の系列が得られた場合の量子系の時間発展は，その系の純粋状態の波動関数 $|\Psi_c(t)\rangle$ として記述できる（共振器外部の放射モードは除去する）．何も光子が検出されない間は，この波動関数は次のような非エルミートな有効ハミルトニアンによるシュレーディンガー方程式により時間発展をする．

$$\hat{H}_{eff}(t) = \hat{H}_1(t) + \hat{H}_2(t) - \sqrt{-1}\kappa\left(\hat{a}_1^\dagger\hat{a}_1 + \hat{a}_2^\dagger\hat{a}_2 + 2\hat{a}_2^\dagger\hat{a}_1\right) \tag{6.4}$$

ここで κ は共振器の損失であり，1 番めと 2 番めの共振器で同じであると仮定してある．時刻 t_r にて光子を検出したとき，量子飛躍 $|\Psi_c(t_r+dt)\rangle \propto \hat{c}|\Psi_c(t_r)\rangle$（$\hat{c} = \hat{a}_1 + \hat{a}_2$）が起きる [285,286]．時刻 t から $t+dt$ の間に量子飛躍（検出器による検出）が起こる確率密度は $\langle\Psi_c(t)|\hat{c}^\dagger\hat{c}|\Psi_c(t)\rangle dt$ で与えられる [285,286]．

6.2.3 理想的な伝送のためのレーザパルス

理想的な量子伝送の条件 (6.3) を満たすように，それぞれの共振器に照射するレーザパルスを設計することを考えてみよう．時間発展に関する必要条件は，量子飛躍（図 6.2 の検出器の計数）が起きない，つまり $\hat{c}|\Psi_c(t)\rangle = 0\,\forall t$ となって，式 (6.4) の有効ハミルトニアンがエルミート演算子になることである．言い換えると，カスケードされた系の中の暗状態 (dark state) になることである．物理的には 2 番めの共振器から波束の反射がないことを意味する．系の状態を次のように展開する．

$$\begin{aligned}|\Psi_c(t)\rangle \;=\; & c_g|gg\rangle|00\rangle \\ & +c_e\Big[\alpha_1(t)e^{-\sqrt{-1}\phi_1(t)}|eg\rangle|00\rangle + \alpha_2(t)e^{-\sqrt{-1}\phi_2(t)}|ge\rangle|00\rangle \\ & +\beta_1(t)|gg\rangle|10\rangle + \beta_2(t)|gg\rangle|01\rangle\Big]\end{aligned} \tag{6.5}$$

このとき理想的な量子伝送 (6.3) が起きる条件は次のようになる．

$$\alpha_1(-\infty) = \alpha_2(+\infty) = 1, \phi_1(-\infty) = \phi_2(+\infty) = 0 \tag{6.6}$$

式 (6.5) の右辺の第 1 項は H_{eff} による時間発展で変化しない．$\beta_{1,2} = (\beta_s \mp \beta_a)/\sqrt{2}$ を満たすように対称係数 β_s と反対称係数 β_a を定めると，以下のような発展方程式が導かれる．

$$\dot{\alpha}_1(t) = g_1(t)\beta_a(t)/\sqrt{2}, \tag{6.7}$$

$$\dot{\alpha}_2(t) = -g_2(t)\beta_a(t)/\sqrt{2}, \tag{6.8}$$

$$\dot{\beta}_a(t) = -g_1(t)\alpha_1(t)/\sqrt{2} + g_2(t)\alpha_2(t)/\sqrt{2} \tag{6.9}$$

ただしレーザ周波数 $\omega_L + \dot{\phi}_{1,2}(t)$ を，$\delta = g^2/\Delta$ かつ

$$\dot{\phi}_{1,2}(t) = \delta\omega_i(t) \tag{6.10}$$

を満たすように選んで AC－シュタルクシフトを補償し，(6.7-6.9) に位相変数が含まれないようにしてある．暗状態条件から $\beta_s(t) = 0$ となるので，式

$$\dot{\beta}_s(t) = g_1(t)\alpha_1(t)/\sqrt{2} + g_2(t)\alpha_2(t)/\sqrt{2} + \kappa\beta_a(t) \equiv 0 \tag{6.11}$$

と，規格化条件

$$|\alpha_1(t)|^2 + |\alpha_2(t)|^2 + |\beta_a(t)|^2 = 1 \tag{6.12}$$

が導かれる．ここで係数 $\alpha_1(t), \alpha_2(t), \beta_s(t)$ は実数である．

ここでの数学的な問題は (6.6)-(6.9), (6.11) を満たすようにパルスの形状 $\Omega_{1,2}(t) \propto g_{1,2}(t)$ を見つけることである．それは，一般的には難しい問題である．なぜなら，微分方程式 (6.7)-(6.9) の解に条件 (6.6), (6.11) を課すことは，未知のパルスの形状についての関数関係を与えることになるからである．われわれは，あるクラスの解を以下の物理的な考察によって構成することにする．まず一つの光子が光学共振器から洩れ出て波束として伝播する状況を考える．この波束を「時間反転」して元の共振器に戻すことができたと仮定しよう．レーザパルス照射のタイミングも時間反転すると，これで原子の元々の (未知の) 重ね合わせ状態を復元することができるだろう．一方，送信側の共振器内の原子を制御することで送り出されるパルスがすでに時間的に対称であるようにできたとすると，受信側の共振器に入る波束はこの時間反転の過程を「模倣」し，そして原子 1 の状態が原子 2 の中に「復元」される．このようにしてこの対称パルス条件

$$g_2(t) = g_1(-t) \quad (\forall t) \tag{6.13}$$

を満たす解を探そう．これは $\alpha_1(t) = \alpha_2(-t)$，$\beta_a(t) = \beta_a(-t)$ を意味する．後者の関係式は，空洞共振器の間に伝播する光子の波束が対称的な形状であることを意味する．

1 番めの共振器のパルスの後半部の形が $\Omega_1(t) \propto g_1(t)$ であったとする[3]．そして，パルスの後半部 $\Omega_1(-t) \propto g_1(-t)\,(t > 0)$ を理想伝送条件 (6.3) を満たすように定めたい．

まず，(6.6), (6.11) により

$$g_1(-t) = -\frac{\sqrt{2}\kappa\beta_a(t) + g_1(t)\alpha_1(t)}{\alpha_2(t)}, \quad (t > 0) \tag{6.14}$$

を得る．この式から，$t \geq 0$ に対して系の時間発展がわかっていると仮定すると，パルス形状は完全に定まる．しかしながらこの時間発展を定めるうえで，未知の $g_2(t) = g_1(-t)$, $(t > 0)$ への依存性が問題になる [(6.7)-(6.9) 参照]．この困難を避けるために，(6.11) を利用して (6.7), (6.9) の $g_2(t)$ への依存性を消去してみよう．すると $t \geq 0$ に対して

$$\dot{\alpha}_1(t) = g_1(t)\beta_a(t)/\sqrt{2} \tag{6.15}$$

$$\dot{\beta}_a(t) = -\kappa\beta_a(t) - \sqrt{2}g_1(t)\alpha_1(t) \tag{6.16}$$

となる．これらの微分方程式を，次の初期条件の下に積分する．

$$\alpha_1(0) = \left[\frac{2\kappa^2}{g_1(0)^2 + \kappa^2}\right]^{\frac{1}{2}} \tag{6.17}$$

$$\beta_a(0) = \left[1 - 2\alpha_1(0)^2\right]^{\frac{1}{2}} \tag{6.18}$$

これらは $\alpha_1(0) = \alpha_2(0)$ および $t = 0$ に対する (6.11), (6.12) から直ちに導かれる．(6.15), (6.16) の解を得られたら (6.12) の規格化により $\alpha_2(t)$ を決定できる．このようにして，$t \geq 0$ に対する (6.14) の右辺に現れるすべての量がわかるので問題を解くことができる．たとえば，$t > 0$ に対して $\Omega_1(t)$ が定数であるような場合に，パルスの形状の解析的な表現を得ることは簡単である．

6.2.4 伝送の不完全性と誤り訂正

以上では，レーザパルスを経由して原子から共振器の場に量子状態を移す伝送の各過程は完全であると仮定し，伝送経路での吸収損失やデコヒーレン

[3] $\Omega_1(t)$ は $\alpha_1(+\infty) = 0$ を満たさないといけない．これは $\Omega_1(+\infty) > 0$ であれば満たされる．この条件は $t > 0$ において (6.14) の分母が 0 にならないことも保証してくれる．

スは考慮しなかった．しかし，現実にはそれらは一定の確率で発生する．ラマンパルスを組み合わせた光学的共振器−光ファイバのシステムは，雑音を伴う量子通信路の一例である．一般には，量子雑音は伝送忠実度を下げ，ノードの間にあったはずの量子相関を破壊する．このような効果は，二つのノードが遠く離れていると特に顕著となる．ここで「遠い」というのは，通信路のコヒーレンス長や吸収長に比較して，ということである．幸いなことに量子誤り訂正 (quantum error correction)[287] とエンタングルメント純化処理 (entanglement purification)[288] が提案されおり，量子雑音やデコヒーレンスに対抗する手段は存在する．8.6 節では上記の量子ネットワークで効率的な誤り訂正をどのように実現するか述べており，その方法で任意のオーダの誤りを訂正できる．これで，比較的短距離では高忠実度の伝送ができる．長距離通信においては，誤り率が指数関数的に上がってしまうので，古典通信の増幅器と同様の役割をもつ量子中継器 (quantum repeater) を考えることになる．

6.3　多粒子エンタングルメント

（*D.Bouwmeeester, J.-W.Pan, M.Daniell, H.Weinfurter, A.Zeilinger*）

6.3.1　Greenberger-Horne-Zeilinger 状態

多粒子間のエンタングルメントは，誤り訂正方式や秘密鍵分配ネットワークなどのほとんどの量子通信方式において，さらには量子コンピュータへの応用において本質的なものである．しかし，いわゆる Greenberger-Horne-Zeilinger(GHZ) 状態などの 3 粒子以上のエンタングル状態を考察したり作ったりする動機は元々別の方面 [289,290] に由来する．具体的には，量子力学が完全な理論であるか否かの論争に由来しているのである．ここではこの原理的・哲学的な議論に細かく触れることを目的とはしないが，読者の理解を助けるため，多粒子エンタングル系がいかに量子情報を蓄え，その量子的性質がなぜ Einstein がいうところの局所性 (locality) とまったく相容れないのか，簡単に解説する．

本節は，3 光子のエンタングルメントの実験的実現を軸に据えて展開するが，この話題はそれ自体量子情報の分野の重要な話題である [291].

6.3.2 局所実在論との矛盾

Greenberger, Horne, Zeilinger は以下のことを示した．あるエンタングルした 3 粒子系に対するある観測の結果の量子力学による予測は，それが確定的（非統計的）な予測を与える場合には，局所実在論 (local realism) と矛盾するのである．[289]-[294]．これは，エンタングルした 2 粒子を用いる，Einstein-Podolsky-Rosen 流のベルの不等式の検証実験が，統計的にのみ局所実在論と矛盾するのとは対照的である [21,23,295,296,297]．

では 3 光子 GHZ 状態の局所実在論との矛盾が，2 光子の場合と比べてどのような意味で強いのだろうか[4]．次の状態を考えてみよう．

$$\frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2|H\rangle_3 + |V\rangle_1|V\rangle_2|V\rangle_3) \tag{6.19}$$

ただし，H, V はそれぞれ垂直偏光，水平偏光を表す．これは，状態 $|H\rangle_1|H\rangle_2|H\rangle_3$（全 3 光子が垂直偏光）と状態 $|V\rangle_1|V\rangle_2|V\rangle_3$（全 3 光子が水平偏光）の量子的重ね合わせである．ここで具体的に与えた状態は，粒子の交換に対して対称であり，それゆえに以下の議論は単純になっているが，同じ議論は 3 光子で「最大限にエンタングルしている」任意の状態についても成り立つ．

状態 (6.19) に対して以下に述べるある測定を行ったときの結果を予測してみよう．すなわち，H/V の基底を 45° 回転した H'/V' と円偏光の基底 L/R（左回り/右回り）で表される基底による偏光測定を各光子に対して行う．これらの基底を最初の H/V を用いて表すと次のようになる．

$$|H'\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \qquad |V'\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{6.20}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle), \qquad |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle) \tag{6.21}$$

$|H\rangle, |V\rangle$ をそれぞれベクトルの $(1,0), (0,1)$ と表示することにより，パウリ行列 σ_z の固有値 $+1, -1$ に相当する固有状態となる．$|H'\rangle, |V'\rangle\big(|R\rangle, |L\rangle\big)$ はパウリ行列 $\sigma_x\big(\sigma_y\big)$ の固有値 $+1, -1$ の固有状態であることも簡単に確かめられる．以下，H'/V' の測定を x 測定，L/R の測定を y 測定と呼ぶことにする．

すると，状態 (6.19) をこれら新しい基底で表すことにより，x 測定や y 測定による測定結果を予測することができる．たとえば，光子 1，2 を L/R の

[4] 2 粒子の場合についても Hardy は，ある状況下では，局所実在論では起こりうると予言される観測結果が，量子力学では決して起きないと予言されることを発見した [298,299]．

円偏光，光子 3 を H'/V' の直線偏光で測定するような yyx 測定を考えよう．測定対象の状態は

$$\frac{1}{2}\ \big(\ |R\rangle_1|L\rangle_2|H'\rangle_3+|L\rangle_1|R\rangle_2|H'\rangle_3 \\ +\ |R\rangle_1|R\rangle_2|V'\rangle_3+|L\rangle_1|L\rangle_2|V'\rangle_3\,\big) \tag{6.22}$$

と表すことができる．この表式はいくつか重要な示唆を与える．第 1 に，光子 1 または 2 の偏光測定をすると，完全にランダムな結果を与える．たとえば，光子 1 が測定により示す結果が R であるか L であるかは 50%である．

第 2 に，この表式には yyx 測定をしたときの測定結果の積が -1 になる項しか現れない．それゆえ，二つの光子の測定結果が与えられると，3 番めの光子の測定結果を確実に予測できる．たとえば，光子 1，2 がどちらも右偏光 (R) を示したとしよう．すると上式の第 3 項から，光子 3 は V' 偏光（測定値 -1）であることがわかる．巡回置換を施すと，同様の表式が xyx 測定と yxx 測定についても得られる．これらの場合も，積が -1 になる測定結果だけが可能である．二つの光子に適当な測定を行うと，その測定結果から円偏光および直線偏光 H'，V' の測定結果が確定する．

これらの示唆を局所実在論から検討してみよう．まず注意すべきことは，これらの予測は光子が空間的に離れているか否かにも関係しないし，時間的な測定順序にも関係しないことである．であるから，ある座標系（たとえば簡単のために光源の座標系）で見たときに，3 個の光子に対する測定が同時に行われる実験を考えよう．Einstein の理論に従うとどんな情報も超光速で伝わることはありえないので，どの光子についても測定結果は，他の光子の測定の仕方とは無関係となる．上記の完全な相関関係を説明できる唯一の説明は次のように仮定することである [289,290,294]．すなわち，それぞれの光子が，考えられているすべての測定に対応した何らかの「実在の要素」(element of reality) を保持しており，その「実在の要素」がそれぞれの測定の結果を決めると仮定するのである．

今ここで xxx 測定，つまり全部の光子に対して直線偏光 H'/V' を測定することを考えてみよう．「実在の要素」の概念を仮定したとき，どんな測定結果がありうるだろうか．状態 (6.19) とその置換を考えると，もしある光子が $H'[V']$ という結果が得られると残りの 2 個の光子はお互い逆回りの [同じ方向の] 円偏光状態にあることになる．では，光子 2 と光子 3 の測定結果が共に

V' だったとしてみよう．すると光子 3 が V' だから，光子 1 と 2 は同じ向きに円偏光している．そして光子 2 が V' だから，光子 1 と 3 も同じ向きに円偏光していなければならない．これらの円偏光が「実在の要素」であるならば，明らかに 3 光子とも同じ向きに円偏光していなければならない．それゆえ，もしも光子 2 と 3 が同じ向きに円偏光しているなら，光子 1 は直線偏光 V' にある．であるから,「実在の要素」の存在を仮定すると，xxx 測定をするときには $|V_1'\rangle|V_2'\rangle|V_3'\rangle$ が一つのありうる測定結果である．同様の議論を進めると，以下の四つの測定結果だけが可能であることが確かめられる．

$$|V_1'\rangle|V_2'\rangle|V_3'\rangle\,,\ |H_1'\rangle|H_2'\rangle|V_3'\rangle\,,\ |H_1'\rangle|V_2'\rangle|H_3'\rangle\,,\ |V_1'\rangle|H_2'\rangle|H_3'\rangle \tag{6.23}$$

これらの局所実在論による予測を，量子力学によるそれと比較してみよう．状態 (6.19) を H'/V' で表示すると次のようになる．

$$\begin{aligned}\frac{1}{2}\ (\ &|H'\rangle_1|H'\rangle_2|H'\rangle_3+|H'\rangle_1|V'\rangle_2|V'\rangle_3\\ +\ &|V'\rangle_1|H'\rangle_2|V'\rangle_3+|V'\rangle_1|V'\rangle_2|H'\rangle_3\,)\end{aligned} \tag{6.24}$$

(6.23) と (6.24) の各項を比較すると，以下のことがわかる．局所実在論から，2 個の光子の測定結果から残りの 1 個の光子の測定結果が確定的に予測できるが，それは量子力学が同じく確定的に予測する結果と正反対なのである．つまり，二つの光子についてのベルの不等式では，局所実在論と量子力学の相違は統計的な予測に現れたが，ここでは統計学が入り込む余地は，どんな古典力学的/量子力学的実験にも付きものの測定誤差のみである．

6.3.3 3 光子 GHZ エンタングルメント生成装置

3 粒子以上のエンタングルメントを生成する実験は，光子 [300]，原子 [301]，イオン（4.3 節参照）について提案されており，一つの分子内の核スピンを局所的に 3 体相関させることに成功している [302]．この節では，空間的に離れた 3 光子間の偏光状態のエンタングルメントをはじめて観測した実験について述べる [291]．この実験に使われた方法は，3.7 節の量子テレポーテーション [76] と 3.10 節のエンタングルメント・スワップ [86] に用いられた技術をさらに発展させたものである．

この実験の基本的なアイデアは，[300] で提案されたように偏光に関してエンタングルした 2 組 (計 4 個) の光子対を，エンタングルした 3 個の光子と 1

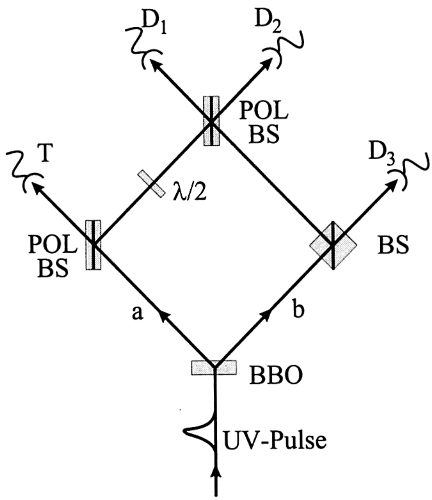


図 6.3　空間的に離れた 3 光子間の Greenberger-Horne-Zeilinger のエンタングル状態を作り出す実験の概念図．検出器 T(triger ditector) で光子が検出されたとき D_1, D_2, D_3 の検出器で検出された 3 光子の間で GHZ 相関が起きている

個の独立した光子に変換することである[5]．図 6.3 は実験装置の概念配置図である．200 フェムト秒パルスの紫外線が BBO 結晶を通過することにより偏光に関してエンタングルした光子対が生成され（3.4.4 項参照），その状態は次のように表すことができる [26].

$$\frac{1}{\sqrt{2}}(|H\rangle_a|V\rangle_b + e^{i\chi}|V\rangle_a|H\rangle_b) \tag{6.25}$$

この状態は $|H\rangle_a|V\rangle_b$ （経路 a の光子が垂直偏光かつ経路 b の光子が水平偏光）と $|V\rangle_a|H\rangle_b$（上記の逆）の重ね合わせを表している．

紫外線パルスが BBO 結晶を通過したとき，このような光子対が 2 対同時に作られることが低い確率で起こる．そのとき 4 個の検出器がそれぞれ 1 個の光子を検出したとしよう（以下，これを 4 重同時検出と呼ぶ）．実験は，4 重同時検出が状態

$$\frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2|V\rangle_3 + |V\rangle_1|V\rangle_2|H\rangle_3) \tag{6.26}$$

[5] エンタングルした粒子対を複数用意して 3 粒子のエンタングルメントを作る方法を応用して，さらに多くの粒子をエンタングルさせることができる．

の計数に対応するように設計されている．この結果は以下のようにして理解できる．4 重同時検出が起きたとしよう．経路 a を通る光子は a にある偏光ビームスプリッタ (Pol BS) を通過しているはずなので，検出器 T(triger ditector) で検出されるためには水平偏光していなければならない．その相方の光子は経路 b 上にあり垂直偏光のはずだから，ビームスプリッタに入って 50%の確率で D_3 に到達し，残り 50%の確率で反射されて次の偏光ビームスプリッタに向かい，反射されて D_2 に到達する．前者の場合，D_1 と D_2 のカウントは 2 番めの光子対によるものである．その光子対の経路 a を通った光子は，偏光ビームスプリッタで反射されているので V 偏光である．その相方の経路 b を通る光子は H 偏光となるが，ビームスプリッタで反射されて（その確率は 50%），最後の偏光ビームスプリッタを通過し D_1 で検出されることになる．したがって，D_2 で検出された光子は H 偏光でなければならない．経路 a から来て最後の偏光ビームスプリッタを通過したはずだからである．この後者の光子の初期状態は V 偏光だったが，22.5° 回転させてある半波長板[6]を通過することにより 45° の偏光となって，50%の確率で D_2 に状態 H で到達するようになっている．以上から，D_3 で検出された光子が T で検出される光子の相方だった場合には，D_1, D_2, D_3 での同時カウントは状態

$$|H\rangle_1|H\rangle_2|V\rangle_3 \tag{6.27}$$

の検出を意味することがわかる．同様の議論で，D_2 で検出された光子が T で検出される光子の相方だった場合には，D_1, D_2, D_3 での同時カウントは，状態

$$|V\rangle_1|V\rangle_2|H\rangle_3 \tag{6.28}$$

の検出を意味することがわかる．

一般には，4 重同時検出に対応する二つの状態 (6.27), (6.28) は干渉性を保ったまま重ね合わさって GHZ 状態を作るとは限らない．両者は原理的には識別可能だからである．まず，検出器への到着時にモードのオーバーラップが損われている可能性があるのみならず，各光子の検出時刻が精確ならば，それでどの状態かを区別できる．たとえば状態 (6.27) は，光子の検出が T と D_3，D_1 と D_2 でおのおのほとんど同時に起こることから識別できる．このような

[6]訳注：入射光の垂直偏光の成分と水平偏光の成分の間に半波長分の光路差を生じさせる．

情報を消去するためには，光子の干渉時間を紫外線パルスの持続時間（約200フェムト秒）より十分長くする必要がある [304]．これは，光子を検出前に狭い帯域幅 (3.6nm) のフィルタに通すことで達成でき，約500フェムト秒の干渉時間が得られる．こうすることで状態 (6.27) と (6.28) の識別可能性を大きく減らすことができ，量子力学の基本原理により，4重同時検出[7]で検出される状態は量子的重ね合わせの状態 (6.26) になる．厳密には，パルスの持続時間とフィルタの帯域幅を無限小にしたときのみこの情報消去は完全で，純粋な GHZ 状態を生成する．しかし詳細な計算 [305] によると，上記の実験パラメータでも明瞭に観測できるエンタングルメントを生成するには十分で，80パーセントの精度を得られる．これは，後に述べる実験結果とも整合する．式 (6.26) に現れる「+」は以下のより厳密な計算で導かれる．2回の下方変換が起こって，次のような状態を生成するとしよう．

$$\frac{1}{2}\left(|H\rangle_a|V\rangle_b - |V\rangle_a|H\rangle_b\right)\left(|H\rangle'_a|V\rangle'_b - |V\rangle'_a|H\rangle'_b\right) \tag{6.29}$$

とりあえず，片方の下方変換で生成される $|H\rangle_{a,b}, |V\rangle_{a,b}$ が，もう片方から生成される $|H\rangle'_{a,b}, |V\rangle'_{a,b}$ と識別可能であるとしておく．式 (6.29) に現れる各項の状態が実験装置を経由して検出器 T, D_1, D_2, D_3 に到達するまでの時間発展は次のようになる．

$$|H\rangle_a \to |H\rangle_T\,, \qquad |V\rangle_b \to \frac{1}{\sqrt{2}}(|V\rangle_2 + |V\rangle_3) \tag{6.30}$$

$$|V\rangle_a \to \frac{1}{\sqrt{2}}(|V\rangle_1 + |H\rangle_2)\,, \quad |H\rangle_b \to \frac{1}{\sqrt{2}}(|H\rangle_1 + |H\rangle_3) \tag{6.31}$$

同様の式は $'$ をつけたほうの状態に対しても成立する．これを式 (6.29) に式を代入した上で，各検出器にそれぞれ1個だけ光子が検出される状態のみを取り出すと次を得る．

$$\begin{aligned}-\frac{1}{4\sqrt{2}}\ \{\ &|H\rangle_T\left(|V\rangle'_1|V\rangle_2|H\rangle'_3 + |H\rangle'_1|H\rangle'_2|V\rangle_3\right)\\ &+ |H\rangle'_T\left(|V\rangle_1|V\rangle'_2|H\rangle_3 + |H\rangle_1|H\rangle_2|V\rangle'_3\right)\}\end{aligned} \tag{6.32}$$

ここで，下方変換で作られた二つの光子対が識別不能であるように実験が行われたとすると，以上から（式全体にかかる「−」を別にして）次の所期の

[7]訳注：原文は，「T の検出で条件付けられた D_1，D_2，D_3 の同時カウント」

結果を得る．

$$\frac{1}{\sqrt{2}}|H\rangle_T\,(|H\rangle_1|H\rangle_2|V\rangle_3+|V\rangle_1|V\rangle_2|H\rangle_3) \tag{6.33}$$

ここでいくつか注意するべきことがある．この配置で生成される全系の状態，すなわち検出直前の状態は，たとえばある検出器に 2 個の光子が入るような項も含み，また，下方変換が 1 回しか起きなかった場合の項も含む．4 重同時検出は，所期の GHZ 状態 (6.33) への射影として働き，それ以外の望まれない状態を除去する．1 個の紫外線ポンプパルスが 4 重同時検出を起こす効率は非常に低く 10^{-10} のオーダである．幸いにも 1 秒間に 7.6×10^7 個の紫外線パルスが生成できるので，150 秒に 1 回 GHZ 状態を得ることができる．なお，3 個や 4 個の光子対の生成は完全に無視できる．

6.3.4 GHZ エンタングルメントの実験的検証

上記の手法で GHZ 状態が得られたことを実験的に証明するには，まず第 1 に，T で光子が検出されたときには $H_1H_2V_3$ と $V_1V_2H_3$ の成分が存在し，かつそれ以外の成分がないことを確かめる必要がある．そのためには，偏光の測定結果の 8 通りの可能性 $H_1H_2H_3$, $H_1H_2V_3$, ..., $V_1V_2V_3$ の起きる比率を比較すればよい．望まれる状態と望まれない状態の比は実験の結果，12:1 であった．これで望まれる二つの状態のみがあることが示されたわけだが，それは GHZ エンタングルメントの必要条件であっても十分条件ではない．実際，二つの状態の統計的混合に過ぎない可能性が原理的には残る．それゆえ，二つの状態の量子可干渉性をもつ重ね合わせであることを示す必要がある．そのために，光子 1 を H と V を二分する方向である角度 +45° の直線偏光を測定する．このような測定は光子 1 を

$$|+45^\circ\rangle_1=\frac{1}{\sqrt{2}}(|H\rangle_1+|V\rangle_1) \tag{6.34}$$

という重ね合わせに射影する．すなわち，状態 (6.33) は次の状態に射影される．

$$\frac{1}{\sqrt{2}}\,|H\rangle_T\,|+45^\circ\rangle_1\,(|H\rangle_2|V\rangle_3+|V\rangle_2|H\rangle_3) \tag{6.35}$$

すなわち,「エンタングルメントがエンタングルしている」[306] ので，光子 2 と 3 は測定後，エンタングルしてしまうのである．さて，光子 2 と 3 の状態

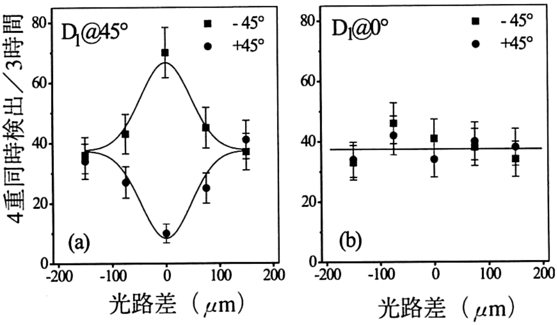


図 6.4　GHZ エンタングルメントの実験的検証．グラフ (a) は，T でカウントがあり，さらに D_1 で +45° 偏光の 1 光子，D_2 で −45° 偏光の 1 光子を検出したときの D_3 の偏光状態を調べた実験結果．二つの曲線は，検出器 D_3 の前にそれぞれ −45° と 45° の偏光板を置いたときの 4 重同時検出が起きた回数を経路 a と b の光路長の差に対する関数として表したものである．光路長の差が 0 のときの差から，確かに GHZ エンタングルメントが得られていることがわかる．比較のため，D_1 の前に 0° の偏光板を置いて実験すると（グラフ (b)），予言されたとおりカウントの差は現れなかった

を +45° の基底で書き換えると

$$\frac{1}{\sqrt{2}}\left(|+45^\circ\rangle_2|+45^\circ\rangle_3-|-45^\circ\rangle_2|-45^\circ\rangle_3\right) \tag{6.36}$$

となる．つまり光子 2 が −45° 方向に偏光しているという測定結果が出たときには，光子 3 も同じ方向に偏光している．$|+45^\circ\rangle_2|-45^\circ\rangle_3$ と $|-45^\circ\rangle_2|+45^\circ\rangle_3$ が式に現れないのは，それぞれが干渉して打ち消しあっているからであり，GHZ 状態 (6.33) の各項が予期されたとおり，干渉性を保って重ね合わさっていることを示している．したがって実験では，検出器 D_1 の前に +45°，D_2 の前に −45°，D_3 の前に +45° または −45° の偏光板をおいて，4 重同時検出を観測する．さらに光子が D_1 と D_2 の前の偏光板に到達する時間の差を変えることができるようになっている[8]．

図 6.4(a) は T でカウントがあり，さらに D_1 で +45°, D_2 で −45° を検出したときの D_3 の偏光状態を調べた実験結果である．

二つの曲線は，D_3 の前に +45°(■) と −45°(●) の偏光板を置いたときに 4

[8] 訳注:干渉性の変化を調べるため．

重検出が起こった回数を経路差の関数として示している．a と b で経路の長さの差が 0 のとき，D_3 の光子は $-45°$ 方向の偏光を示しており，GHZ 状態に対する量子力学の予言に沿うものである．経路長の差が 0 でないときには，経路 a を通って 2 番めの偏光ビームスプリッタに到達した光子と，b を通過した光子が識別できるようになる．それゆえ，経路差を増やしていくと 3 粒子状態の量子的重ね合わせが徐々に失われていく．

また，経路長の差が 0 のとき，D_2 の光子が $-45°$ 偏光に射影されると，D_1 と D_3 の 2 個の光子がエンタングルした状態に射影されるわけであるが，これも同様に実験データから確かめることができる．これらは，状態が真の GHZ 状態であるときのみ成り立つ．

追加的な確認実験として，D_1 の光子を $0°$ 偏光（すなわち V 偏光）に射影した場合の実験を行った．生成された状態が GHZ 状態 $(1/\sqrt{2})(H_1H_2V_3+V_1V_2H_3)$ ならば，V_2H_3 のみが残るので，45° 方向の偏光を計っても相関は現れない．図 6.4(b) にその実験結果が示されている．実験データから確かに 2 光子間に相関がないことがわかり，空間的に離れた 3 光子が GHZ エンタングルメントしていることを確かめることができた．

この GHZ エンタングルメントは，4 重同時検出のときのみ起こることに注意しよう．4 重同時検出は GHZ 状態 (6.26) への射影と，GHZ 状態に対するある特定の測定という二つの役割を担っている．

このような状態発生源が局所実在論の検証に使えるのか，という疑問が起こるかもしれない．実際，同じ疑問が光子の識別不能性を利用したベルの不等式検証実験に関して起きていた [307,308]．これらの実験は長距離の量子力学的相関を作るのに成功したのだが，実験が理想的に行われた場合ですら，決して局所実在論に対する真の検証にはならないと従来信じられてきた [309,310]．しかし Pspescu，Hardy，Zukowski[311] はこの一般に信じられた説は正しくないことを示した．つまりこの実験は，（光子検出器の不完全さが原因の抜け穴を別にして）局所実在論に対する正しい検証法になっている．同じような推論に従い，Zukowski[312] は上記の GHZ エンタングルメント発生装置が 3 粒子の局所実在論の検証に使えることを示した．GHZ の局所実在論に関する議論は，本質的には事象の検出のみに依存しており，背後にある量子状態についての知識は必要としない．つまり 4 重同時検出の上記の議論のみを考えれば十分で，他の項の寄与は完全に無視してよい．

6.3.5　局所実在論 v.s. 量子力学の実験による検証

前節の GHZ エンタングルメント状態発生源を用いて，局所実在論と量子力学の矛盾を実験的に論じるには以下のようにすればよい．まず，6.3.2 項で考えたように yyx, yxy, xyy 測定を行う．これら三つの実験で，それぞれの実験の可能な測定結果は 2^3 通りある．

図 6.5 は実験的に得られた 3×2^3 通りの測定結果の確率分布である．ここでは，6.3.2 項で状態 (6.19) についてなされた議論と比較するために (6.26) の 3 番めの光子の偏光を定義し直しており，$|H\rangle_3$ と $|V\rangle_3$ を入れ替えてある．

図 6.5 の最大値と最小値からビジビリティ(visibility) を $(\langle\text{max}\rangle - \langle\text{min}\rangle)/(\langle\text{min}\rangle - \langle\text{max}\rangle) = .71 \pm 0.04$ と計算できるので，0.71 ± 0.04 の精度で存在すべき項と存在すべきでない項が特定できる．ビジビリティが 1 でないことは，ポンプパルスとフィルタの帯域幅が無限小でないことにより主に説明できる（6.3.3 項参照）．しかし，局所実在論対量子力学の原理的検証としては，図 6.5 をブラックボックスから出てきた 3 粒子のアンサンブルに対してなされた測定の結果と考えるのが必須とはいわないまでも，適切であろう．こうすると，GHZ エンタングルメント状態生成源の諸性質は，以下の局所実在論を反駁する議論でまったく効いてこない．局所実在論の立場に立って，各粒子の観測結果は他の空間的に離れた粒子の観測結果の影響を受けないとすると，図 6.5 の実験結果から（6.3.2 項での議論に従い）xxx 測定の測定結果を予測できる．その予測は図 6.6(a) に示されている．

量子力学の立場に立つと，予測は図 6.6(b) のようになる．これらの予測は，図 6.5 の実験結果が確度 0.71 で 3 粒子エンタングルメントの存在を示している，という議論から導かれている．果たして xxx 測定の実験結果は図 6.6(c) の通りである．

実験結果は，局所実在論の予測とは大きく異なり，量子力学の予測にまったく一致するものであった．実際，実験の誤差の範囲で量子力学の予測 (6.24) に一致し，局所実在の予測する結果 (6.23) は 起きなかった．以上の意味で，この実験は局所実在論の不等式を用いない 3 粒子テストのはじめての例となった [313].

局所実在論者は次のように言うかもしれない．どんな実験でも，要求された完全な相関条件を満たすことはありえないので，GHZ の予言は完全には実

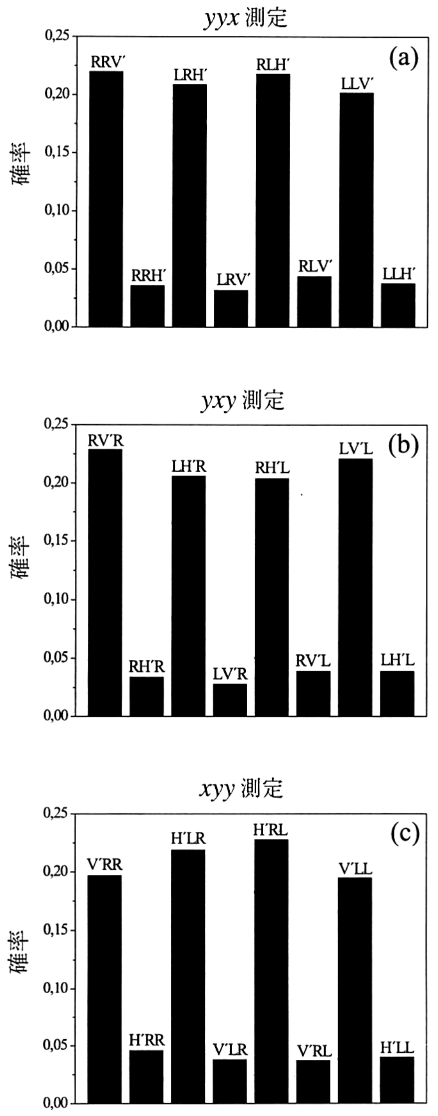


図 6.5 (a)yyx 測定，(b)yxy 測定，(c)xyy 測定で生じうる結果の確率分布を実験により求めたもの

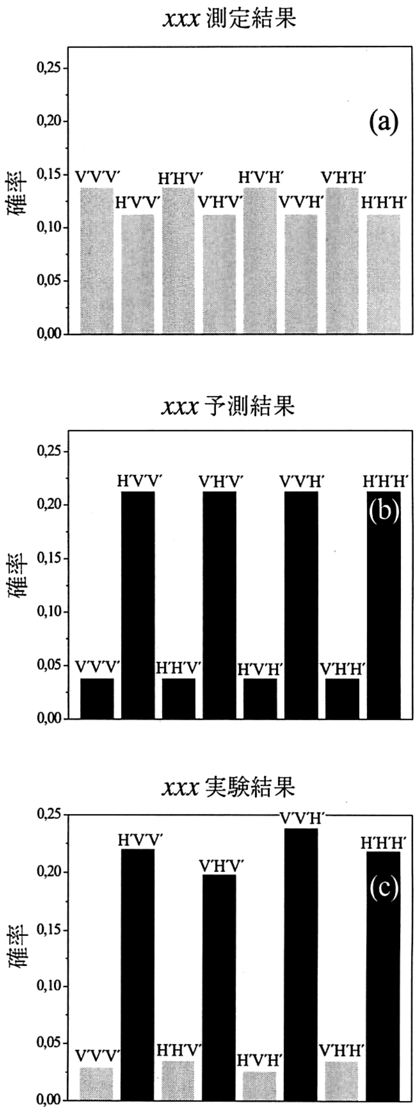


図 6.6　(a) 局所実在論が予測する xxx 測定の結果（図 6.5 の実験結果に基づく）．(b) 量子力学が予測する結果．(c) 実際の実験による結果．局所実在論の予測とは大きく異なるが，量子力学の予測とは実験の誤差内で一致する

験室でテストされ得ず，したがって，上記の議論は納得できない．これに対しては，N–粒子 GHZ 状態でのベル型の不等式が多数考案された [314]-[316]．これらは，量子力学の予測では，GHZ 状態が N の増加に従い指数関数的な超過で不等式を破ることを示した．たとえば，Mermin は 3 粒子の GHZ 状態に対する最適化されたベル型の不等式を次のように与えた．

$$|\langle xyy\rangle + \langle yxy\rangle + \langle yyx\rangle - \langle xxx\rangle| \leq 2 \tag{6.37}$$

ここで，たとえば $\langle xyy\rangle$ は粒子 1,2,3 に対するそれぞれ x, y, y 測定の測定値[9]の積の期待値である．このベルの不等式を破るのに必要なビジビリティは50%である [314]．上記の実験では鮮明度は約 70% であったから，明らかにこの 50% を超えている．実験結果を不等式 (6.37) の左辺に代入すると

$$|\langle xyy\rangle + \langle yxy\rangle + \langle yyx\rangle - \langle xxx\rangle| = 2.83 \pm 0.09 \tag{6.38}$$

である．つまり，実験結果は標準偏差の 9 倍の大きさの超過で不等式 (6.37) を破り，局所実在論との矛盾がはっきりと現れている．それでもなお，上記のテストは局所実在論への最終宣告とはならないことを注意しておく．光子検出効率が高くないことや，複数の検出が space-like な関係にない，などいくつかの“抜け穴 (loophole)”があるからである．

6.4 エンタングルメントの定量化

（*V. Vedral, M.B. Plenio, P.L. Knight*）

6.4.1 シュミット分解とフォンノイマン・エントロピー

量子複合系はいくつかの部分量子系で構成される．それらの部分系がエンタングルしているとき，それぞれの部分系ごとに一つの状態ベクトルを割り当てることができない．そのような複合系の簡単な例は 2 個の偏光した光子がエンタングルしたものである（3.4.4 項参照）．この複合系を数学的に記述すると次のようになる．

$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2\right) \tag{6.39}$$

[9]**訳注**：原文では eigenvalue（固有値）となっているが，意味をとりやすくするために敢えて言葉を入れ換えた．

この複合系の性質は，2 光子の偏光の方向がどんな軸に対しても直交している，といったものである．一見して，式 (6.39) からどちらの各光子も一つの量子状態（偏光状態）ベクトルを決められないことがわかる．この状況で何かを言えたとしても，それは 1 個の光子を測定したときにたとえば垂直偏光 ($|V\rangle$) であることがわかれば，もう片方の光子は水平偏光 ($|H\rangle$) であるといったことである．しかし，一般の複合系の場合にはこのような言い方ができるとも限らない．このような状況を扱うため，シュミット分解 [317] を導入する．これは数学的に便利であるだけでなく，二つの部分系の間の相関関係について深い知見を与えてくれる．

2 個の部分系 A と B（一方は N 次元で他方は M 次元．ただし $M \leq N$）の任意の状態をシュミット分解すると

$$|\Psi_{AB}\rangle = \sum_{i=1}^{M} c_i |u_i\rangle |v_i\rangle \tag{6.40}$$

となる．ただし，$\{|u_i\rangle\}$ は部分系 A の直交基底であり $\{|v_i\rangle\}$ は部分系 B の直交基底である．2 個の部分系が全体として純粋状態であるときの相関関係を理解するための基本的な性質が 2 点ある．

- それぞれの部分系に制限した密度行列は，シュミット基底によって対角化され，さらに同じ正のスペクトルをもつ．ここで部分系 A に制限した密度行列というのは全体の状態 $\rho_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}|$ を B のすべての状態にわたってトレースして得られた状態であり

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB} := \sum_q \langle v_q|\rho_{AB}|v_q\rangle = \sum_p |c_p|^2 |u_p\rangle\langle u_p| \tag{6.41}$$

  である．同様に $\rho_B = \sum_p |c_p|^2\, |v_p\rangle\langle v_p|$ となる．
- 片方の部分系が N 次元系であれば，もう一つの部分系の N 個を越えた直交する状態とエンタングルすることはできない．

ここで，一般に 3 体以上のエンタングルした系はシュミット分解はできないことを指摘しておこう．数学的な詳細は [318] に書かれているが，説明のために例として 3 体のエンタングルメントした系を考えよう．ここで，1 体を観測すると瞬間的かつ確定的に残り 2 体の状態を知ることができるような形

で一般の系を記述したいわけである．しかし，一般にはこれは不可能である．1体の観測によって，結果的に残りの2体がエンタングルすることができるからである（6.3.4項参照）[10]．4体以上ならさらに難しくなるのは明らかだろう．同じようなことが混合状態（密度行列が $\rho^2 \neq \rho$ となっていない，すなわち巾等でない）については2体以上ですら起こり，一般にシュミット分解できない．シュミット分解の存在のおかげで，2体の純粋状態はエンタングルメントは理解しやすく定量化が容易であるけれども，混合状態または3体以上の場合は問題が複雑になってしまう．

2体の純粋状態についてエンタングルメントを定量化するために，以下のような量子系の状態の「不確実さの尺度」を導入する．

定義 密度行列 ρ で表される量子系のフォンノイマン・エントロピーは次のように定義される [319].

$$S_N(\rho) := -\mathrm{Tr}(\rho \ln \rho) \tag{6.42}$$

（混乱の恐れがない限り添字の N は省略する.）A と B の間のエンタングルメントは以下のように理解できる．系 B に制限した密度行列を ρ_B とすると，系 A を観測する前の系 B の不確実さの量は $S(\rho_B)$ である．観測をしてしまうと，たとえば系 A が $|u_i\rangle$ という観測結果により系 B は $|v_i\rangle$ とわかるので，不確実さはなくなってしまう．このとき得た情報量は $S(\rho_B) = S(\rho_A)$ である．したがって，個々の系に制限した密度行列が「最大限に混合している状態」を表すとき，A と B は最大限にエンタングルしているといえる．2体の量子ビットの場合には，最大エンタングル状態はたとえば $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ である．

この純粋状態のエンタングルメントの尺度については，さらに別の物理的な解釈ができる．純粋状態 $a|00\rangle + b|11\rangle$ から局所的な操作[11]で取り出せるエンタングルメントの量[12]は，部分トレースをとった状態のエントロピー以下であることが示せる [117] [13]．一方，$a|00\rangle + b|11\rangle$ からなるアンサンブルを局

[10]訳注：ここで 6.3.4 項の GHZ 状態を例とするのは正しくない．確かに GHZ 状態はある基底で測定すると残りの 2 体がエンタングルする．しかし，GHZ 状態は「シュミット分解」(6.19) をもつのである．

[11]訳注：ここで局所的な操作といっているが，実は次の節でもあきらかになるように，二つの系の間の古典的な情報のやりとりも許している．

[12]訳注：最大エンタングル状態 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ の数のことを，エンタングルメントの量といっているようである．

[13]訳注：正確には，状態 $a|00\rangle + b|11\rangle$ からなるアンサンブルから，状態一つあたり，何個の最大エンタングル状態を取り出せるかを考える．

所操作のみで作り出すには，平均すると状態一つあたり，縮約エントロピーだけのエンタングルメントを前もって共有している必要がある[14].

混合状態についてはシュミット分解が存在しないので，縮約エントロピーはよいエンタングルメント尺度ではなくなる．この場合，エンタングルメントを定量化するにはエンタングルメント純化処理を用いればよい．まず純化処理を一般的に定式化して，それに基づいて 3 種類の異なるエンタングルメント尺度を導入する．

6.4.2　エンタングルメントの純化処理

エンタングルメントの弱い状態のアンサンブルから，強くエンタングルメントしている状態の部分アンサンブルを抽出する処理をエンタングルメント純化処理と呼び，次のような三つの過程で構成される．

1. 局所一般測定 (LGM; Local general measurements)：A,B の 2 者がそれぞれ別々に行う測定であり，完備性の条件 $\sum_i A_i^\dagger A_i = I$ と $\sum_j B_j^\dagger B_j = I$ を満たす作用素族 $\{A_i\}_i, \{B_j\}_j$ で記述される．これらを両方行う作用は $\{A_i \otimes B_j\}_{ij}$ と書ける．この操作自体も $\sum_{ij}(A_i \otimes B_j)^\dagger (A_i \otimes B_j) = I$ を満たす完備な一般測定であり，明らかに局所的なものとなっている．任意の LGM は，付加系と相互作用させた上でその付加系を測定することで実現できる．図 6.7 参照．
2. 古典通信 (CC: Classical Communication)：これは，部分系 A と B で行なう操作は相関しうることを意味する[15]．そして，全系 $A+B$ の完備測定 (complete measurement) として記述され，(LGM とは異なり,) それぞれの系の作用素の直積の和に分解できない．A と B に共有される変換前の状態 ρ_{AB} に対して "LGM+CC" を行うと，状態の変換は次のような形になる．
$$\rho_{AB} \to \sum_i A_i \otimes B_i \, \rho_{AB} \, A_i^\dagger \otimes B_i^\dagger. \tag{6.43}$$
つまり，A と B の両者による操作が " 相関 " している．
3. 選択 (PS: Post Selection)：この操作は上記の LGM,CC の後に行われる (図 6.8 参照)．数学的には，完備ではない一般測定に相当しており，(6.43)

[14]訳注：この言明と先の言明が成り立つには，本当は $S(\rho)$ の定義で対数の底を 2 にしておく必要がある．
[15]訳注：ここで相関は，古典相関を意味する．

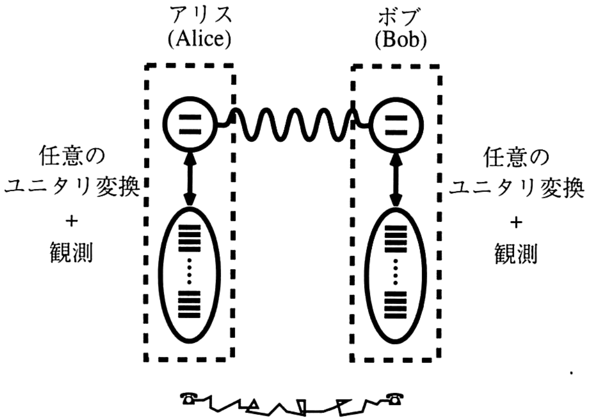


図 6.7 エンタングルメント純化処理では，点線の四角に示されている局所一般測定をゆるす．この操作は，ある多準位系が付与されて元の量子ビットと相互作用した後に多準位系がどの状態にあるか測定する．この方法は測定の最も一般的なものである．さらに，図の電話の記号で表されている古典通信を行ってよい

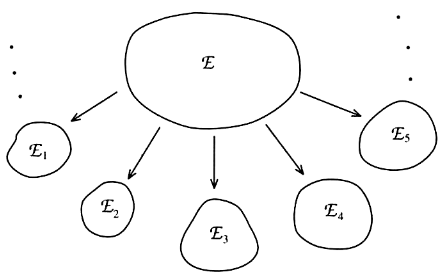


図 6.8 局所測定によるアンサンブルの選択がエンタングルメント純化において重要である．処理前のアンサンブル $\mathcal{E}$ は部分アンサンブル $\mathcal{E}_i$ に分解される．それらのうちいくつかが処理前のアンサンブルよりも高いエンタングルメントを得る

のいくつかの項を落した形になっている．それに対応して，新しいアンサンブル（元のアンサンブルの部分アンサンブル）の密度行列は，規格化しなおさなければならない．A_i と B_j に相当する観測結果を得た場合

だけを取り出すと，その部分アンサンブルの状態は

$$\hat{\rho}_{AB} \to \frac{A_i \otimes B_j\, \rho_{AB}\, A_i^\dagger \otimes B_j^\dagger}{\mathrm{Tr}(A_i \otimes B_j\, \rho_{AB}\, A_i^\dagger \otimes B_j^\dagger)} \tag{6.44}$$

となる．ここで分母は規格化定数である．

上記の操作と，それらの組合せでできる操作を純化処理と呼ぶ．どの操作も局所的であることに注意されたい．これは全体の集団のエンタングルメントは決して増えないことを意味する．しかし古典通信を許しているので，全アンサンブルでみても，古典相関は増加し得る．

状態 ρ_{AB} がエンタングルしていない（もしくは「分離可能」である），ということを次で定義する．

$$\rho_{AB} = \sum_i p_i\, \rho_A^i \otimes \rho_B^i. \tag{6.45}$$

ただし，ここで $\sum_i p_i = 1$ かつすべての i について $p_i \leq 0$ としてある．このように状態が表せないとき,「エンタングル」しているという．各 ρ_A^i, ρ_B^i が固有ベクトル分解できるので，式 (6.45) の右辺おいて $\rho_A^i \otimes \rho_B^i$ は純粋状態であると仮定しても構わない．つまり，条件に ${\rho_A^i}^2 = \rho_A^i, {\rho_B^i}^2 = \rho_B^i$ を付け加えてもよいことを意味する．このことはこの 6.4 節の後のほうで用いる．

6.4.3　エンタングルメントの尺度であるための条件

ある種の状態からは LGM+CC+PS によって最大エンタングル状態を抽出できることが証明できるが [50]，エンタングルしていない状態からはエンタングルメントはもちろん抽出できない．しかし，逆は一般に正しくなく，エンタングルしていても最大エンタングル状態を抽出できるとは限らない [320]．では，ある状態が与えられたとき，どれだけエンタングルメントを含んでいるといえるのだろうか．この問題は，どんな物理的状況でエンタングルメントの量を特徴付けるかをはっきりさせないと，明確に定義されない．このことは，すぐ後でわかるように，エンタングルメントの尺度は一つだけではないことを示唆する．三つの異なるエンタングルメントの尺度を定義する前に，まず，すべての尺度が満たすべき四つの条件 [321,322] を述べる[16]．

[16]訳注：これらの条件は，現在は一般的でない．特に,「連続性」といわれる条件が挙げられておらず，E1 が強過ぎる．詳しくは以下の文献を参照のこと．M. J. Donald, M.l Horodecki, O. Rudolph, *Journal of Mathematical Physics* 43 (2002) 4252-4272, http://xxx.lanl.gov/abs/quant-ph/0105017.

E1. $E(\sigma)=0$ であることと σ が分離可能なことは同値.

E2. 局所ユニタリ変換は $E(\sigma)$ を変えない．つまり $E(\sigma)=E(U_A{\otimes}U_B\,\sigma\,U_A^\dagger{\otimes}U_B^\dagger)$ が成り立つ.

E3. LGM+CC+PS はエンタングルメントの期待値を増やさない．つまり，$\{V_i\}_i$（$\sum V_i^\dagger V_i=I$）で現れる LGM + CC + PS に対して，次の式が成り立つ.

$$\sum \operatorname{Tr}\sigma_i\, E\left(\frac{\sigma_i}{\operatorname{Tr}\sigma_i}\right)\le E(\sigma) \tag{6.46}$$

ここで，$\sigma_i=V_i\sigma V_i^\dagger$ とした.

E4. 純粋状態に対しては，縮約した密度行列のエントロピーに一致する.

条件 E1 は，分離可能状態のみがエンタングルメント量が 0 であることを保証する条件である．E2 は，局所系の基底の変更はエンタングルメントの量に影響を与えないことを保証している．E3 は，古典通信と組み合わせた局所測定でエンタングルメントが増える可能性を排除するための条件である．ここで，終状態についての知識が観測者に得られていることを考慮している．つまり状態 σ が n 個あるとき，純化処理でどの $m_i=n\times\operatorname{Tr}(\sigma_i)$ 個のペアが状態 σ_i にあることがわかっている．したがって，σ_i で記述される可能な部分アンサンブルのそれぞれのエンタングルメントを利用できる．明らかに，E3 で述べたように変換後の全体のエンタングルメントは，最初のエンタングルメントを超えない．もちろん，これはある部分アンサンブルにおいてエンタングルメントが大きくなる可能性を排除しない．E4 は，純粋状態のエンタングルメント量の尺度が一意的であることとの整合性の条件である．われわれは E1-E4 に従った三つの異なる尺度を導入する．特別な目的により E4 の条件を外すこともあり，その具体例はこの節の後のほうで与える.

最初に，形成エンタングルメント量 (entanglement of formation) [323] について述べよう．ベネットらは ρ に対する形成エンタングルメント量を次のように定義した[17].

$$E_f(\rho):=\min\sum_i p_i S(\rho_A^i) \tag{6.47}$$

ただし $S(\rho_A)=-\operatorname{Tr}\rho_A\ln\rho_A$ はフォンノイマン・エントロピーであり，式の右辺の min は $\rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|$ を満たすあらゆる分解についての最小化であ

[17]訳注：原文では E_c であるが，現在の慣例では E_f が一般的であり，E_c は別の意味に用いられる.

る ($\rho_A^i = \mathrm{Tr}_B|\psi_i\rangle\langle\psi_i|$)．$E_f$ は LGM+CC で増えないので，E1-E4 をすべて満たす [323]．この尺度の物理的な意味は，与えられた状態を作り出すのに必要な 1 重項状態の個数である[18]．最近，$C^2 \otimes C^2$ に住んでいる状態については，min の形を用いないで代数的な操作で計算できる閉じた式が見つかった [324].

この尺度と関連するものとして抽出エンタングルメント量 (entanglement of distillation) がある [323]．これは状態 σ から純化処理を用いてどれだけの 1 重項状態を取り出すことができるかをもって，エンタングルメントの尺度とするものである．特定の純化処理の効率に依存していないように，ある一般的な純化処理の中で最適な効率をもってこの量を定義する．抽出エンタングルメント量の計算は形成エンタングルメント量よりもさらに困難であるが，後でその上限を与える．

ここでエンタングルメントの 3 番めの尺度を与えよう．この方法で定義される尺度は，エンタングルメントのよい尺度すべてを網羅するかもしれない．これは上界を与えているという意味で E_d と密接な関連がある [322].

もし $\mathcal{D}$ がエンタングルしていない状態の集合だとすると（図 6.9 参照），状態 σ に対して次のように定義される．

$$E(\sigma) := \min_{\rho \in \mathcal{D}} D(\sigma||\rho) \tag{6.48}$$

ただし，D は状態 ρ と σ の間の適当な「距離」であって[19]，$E(\sigma)$ が条件 E1-E4 を満たすようにする．

ここで重要なのは，どのような $D(\rho||\sigma)$ の条件が E1-E4 を満たす尺度を生成するかである．必要十分条件は知られていないが，十分条件は知られている [321]．ここでは E1-E4 を満たす尺度を一つ，E1-E3 のみを満たす尺度を一つ紹介するが，数学的な詳細には触れない（必要ならば [322] を見よ）．

---

[18]**訳注**：この記述は誤り．与えられた状態をつくり出すのに必要な 1 重項状態の個数は，消費エンタングルメント量 (entanglement cost) といわれ，$E_c(\rho)$ などと表され，$E_c(\rho) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho^{\otimes n})$ という式で E_f と結び付く．ただし，$E_c = E_f$ が成立するとする有名な予想がある．がしかし，もちろん証明はなく，否定的な材料もある．なお，ここで 1 重項状態とあるが，2 次元の最大エンタングル状態なら何でもよい．以下，本節の記述は現在から見ると問題のある点が多く，時に断りなく修正してある．

[19]**訳注**：原文には distance であって metric ではないと書かれている．前後関係から，metric といっているのは，数学で普通いう距離，すなわち対称性と三角不等式を満たす距離のことをいい，distance には特にそういう制限をおいていないと推測される（ただし，そのような用語法は決して一般的でない）．たとえば，後で用いられる相対エントロピーは対称でなく，普通の意味の三角不等式を満たさない．

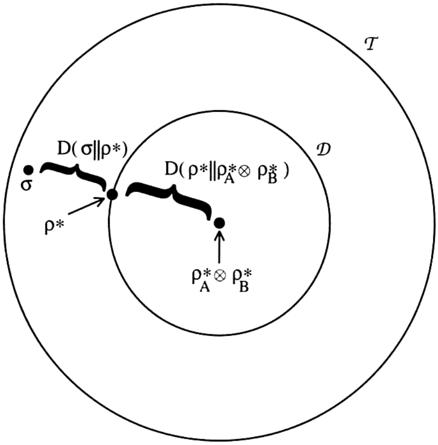


図 **6.9** $\mathcal{T}$ は，外円で表されている密度行列の集合である．$\mathcal{D}$ は，内円で表されているエンタングルしていない状態の集合である．状態 σ はエンタングルしており，σ^* は $D(\sigma||\rho)$ を最小化する ρ である．したがって，$D(\sigma||\rho)$ は σ の量子相関の量を表していると言える．状態 ρ^*_A, ρ^*_B は ρ^* をそれぞれ A, B の系に縮約したものであり，$D(\rho^* \,||\, \rho^*_A \otimes \rho^*_B)$ は σ のもつ相関のうち古典的な部分と言える

6.4.4 密度行列間の二つの「距離」

第 1 に，量子相対エントロピー $S(\sigma||\rho) := \mathrm{Tr}\{\rho(\ln\sigma - \ln\rho)\}$ を (6.48) の $D(\sigma||\rho)$ に代入して定義される尺度は E1-E4 を満たす [322]．ただし量子相対エントロピーは非対称，つまり $S(\sigma||\rho) \neq S(\rho||\sigma)$ で，しかも三角不等式を満たさないので本当の意味での距離とは言えない．これについては次の 6.4.5 項で明らかにする．どうしてエンタングルメントの尺度が $\min_{\rho\in\mathcal{D}} S(\rho||\sigma)$ では定義できないのか気になるかもしれない．これは，量子相対エントロピーのこの非対称から，別の尺度を与える．しかし，この定義では最大エンタングル状態に対して値が無限大になってしまう点が問題である．このことは自然な統計学的意味をもつのだが（次節参照），この量を何らかの物理的に意味のある操作（純化処理など）と関係付けるのは困難である．主に以上の理由によって，この方式による定義は今後考えない．以後，量子相対エントロピーで定義される尺度を「エンタングルメントの相対エントロピー」と呼ぶ．この尺度に関する重要な定理を次に示す（証明は [322]）．

定理　純粋状態に対してエンタングルメントの相対エントロピーは，部分トレースをとった密度行列のフォンノイマン・エントロピーに一致する．

純粋状態に対してフォンノイマン・エントロピーはエンタングルメントのよい尺度としてすでに知られているので，これは物理的によい性質である．

以下に述べるように，形成エンタングルメント量 E_f はエンタングルメントの相対エントロピー以上である．この結果は，後で述べるように次の重要な事実を導く．すなわち，与えられたエンタングル状態を得るために必要なエンタングルメントの量は，後でエンタングルメント抽出で回収できるエンタングルメントを上回るのである[20]．

定理 $E_f(\sigma) \geq E(\sigma)\big(= \min_{\rho\in\mathcal{D}} S(\sigma||\rho)\big)$

ベル対角状態に対しては形成エンタングルメント量とエンタングルメントの相対エントロピーが簡単に計算できることを付け加えておこう [321]．そして，ベル対角状態では 形成エンタングルメント量はエンタングルメントの相対エントロピーよりも真に大きい．

エンタングルメントの相対エントロピーの陽な形は知られておらず，与えられた σ に対して ρ^* を見つけるためには，コンピュータによる探索が必要となる．しかしながら，次の 6.4.5 項で述べるようにスピン 1/2 の粒子系に対してはエンタングルメントの相対エントロピーを非常に効率よく計算できる．

E1-E3 を満たしながら E4 を満たさない尺度の例は，Bures の距離を用いて与えられる．Bures の距離は，いわゆる忠実度（もしくは Uhlmann の遷移確率）と呼ばれる $F(\sigma,\rho) := \left[\mathrm{Tr}\{\sqrt{\rho}\sigma\sqrt{\rho}\}^{1/2}\right]^2$ を用いて $D_B(\rho||\sigma) := 2 - 2F(\sigma,\rho)$ と定義される．量子相対エントロピーのときのように，いくつかの簡単な状態についてはこのエンタングルメントの尺度を計算できる．たとえば，最大限にエンタングルした状態には $E = 1$ である．同様にして，一般的な純粋状態 $\alpha|00\rangle + \beta|11\rangle$ に対しては[21] $E = 4\alpha^2\beta^2$ を与える．一般にはエンタングルメントの相対エントロピーの場合と同じくコンピュータによる探索が必要となる．次の 6.4.5 項ではコンピュータによるエンタングルメントの相対エントロピーの数値計算について述べる．

---

[20] この記述は誤り．理由は先に述べたように，消費エンタングルメント量が形成エンタングルメント量を下回る可能性を否定できないので．

[21] 2 個の 2 準位系の場合，これはシュミット分解を考えると最も一般的な形である [317]．

6.4.5 スピン 1/2 の 2 粒子系に対する数値計算

エンタングルメントの相対エントロピーには閉じた解析的な公式が知られていないので，一般的な量子状態 σ に対しては数値計算による探索に頼る必要がある．このような探索は凸解析 [325] の結果を用いると効率的に行える．以下では，基本的な定義と重要な結果を一つずつ凸解析から導入する [325]．これより以降はエンタングルメントの相対エントロピーのみを議論するが，以下に述べることの多くはより一般の場合にも当てはまる．非エンタングル状態の式 (6.45) による分解をする際，添え字の数が有限で済むことを意味する次の定理は，最小化問題を解く際に重要な役割を果たす．

カラテオドリ (Caratheodory) の定理 $A \subset \mathbf{R}^N$ とする．co(A) を A の凸包とすると，$x \in \mathrm{co}(A)$ に対して $x = \sum_{n=1}^{N+1} p_n a_n$ を満たすような $p_n \geq 0$ と $a_n \in A (n = 1, \ldots, N+1)$ が存在する．ただし $\sum_{n=1}^{N+1} p_n = 1$ とする．カラテオドリの定理の直接的な結果は，エンタングルしていない状態 $\mathcal{D}$ の任意の状態は高々$(\dim(H_1) \times \dim(H_2))^2$ 個の純粋状態の和で書けるということである．つまり 2 個のスピン 1/2 の粒子対は式 (6.45) の右辺の高々16 項の総和で書くことができる．さらに，1 粒子の純粋状態は 2 個の実数パラメータで記述できるので，$15 + 16 \times 4 = 79$ 個の実パラメータがあれば，エンタングルしていない状態はすべて記述できる．なお，この効率的な数値計算は，与えられた状態 σ [22]がエンタングルしていない状態か否か，すなわち (6.45) の形か否かを判定する，新たな方法を与える．すでにある手法としては，それはペレスとホロデッキ家の人々により与えられた次の条件がある．すなわち，部分転置した結果が正定値行列であることが非エンタングル状態の必要十分条件である（[326] の 2 番めと 3 番めを参照）．この判定法は 2 個のスピン 1/2 粒子系か，スピン 1/2 粒子とスピン 1 粒子から成る系にしか使えないので，その他の場合は上記のコンピュータによる探索に頼ることになる．

最後に，エンタングルメント尺度の性質として期待されるべき重要な性質，すなわち「加法性」について触れておこう．これは次の式で書ける．

$$E(\sigma_{12} \otimes \sigma_{34}) = E(\sigma_{12}) + E(\sigma_{34}) \tag{6.49}$$

[22]訳注：原文では “a given state σ of two spin-1/2 systems” とあるが，その場合はすぐ後に述べられているように，部分転置の手法が有効であるので，エンタングルしているか否かの判定を数値計算に頼る必要はない．そこで，前後の意を汲んで σ は与えられた任意の状態とした．

ただし左辺では，系 1+3 対系 2+4 の間のエンタングルメントを考えている．左辺の厳密な定義は

$$E(\sigma_{12} \otimes \sigma_{34}) = \min_{p_i, \rho_{13}, \rho_{24}} S(\sigma_{12} \otimes \sigma_{34} || \sum_i p_i \rho_{13}^i \otimes \rho_{24}^i) \tag{6.50}$$

である．なぜ，(6.50) を考える必要があるのであろうか？ $\sigma_{12} \otimes \sigma_{34}$ から相対エントロピーが最小なエンタングルしていない状態は，$\sum_i p_i \rho_{13}^i \otimes \rho_{24}^i$ の形の状態であると思うかもしれない．しかし，アリスとボブは任意の局所ユニタリ変換を行うことができる．これは，明らかに系 1 と 2，3 と 4 の間にエンタングルメントを作り，それゆえ (6.50) を考えなければならないのである．純粋状態の場合には，エンタングルメントの尺度がフォンノイマン・エントロピーに帰着するので，加法性はもちろん成り立つ．一般の場合については，解析的な証明はまったくなく，加法性は予想にとどまっている．しかしながらスピン 1/2 粒子の場合，われわれの数値計算では反例は見つかっていないので加法性は成り立つと思われる[23]．加法性の性質を仮定すると，条件 E3 により，エンタングルメントのエントロピーは任意のエンタングルメント純粋化処理の効率度の上限を与える．もしも n 個の状態 σ から m 個の 1 重項状態が得られたとすると

$$n \times E(\sigma) \geq m \ln 2 \tag{6.51}$$

となるので，効率 m/n は $E(\sigma)$ で抑えられている．$E(\sigma)$ は形成エンタングルメント量よりも小さいこともあるので，形成エンタングルメント量と抽出エンタングルメント量は必ずしも一致しない．

6.4.6　エンタングルメント尺度の統計的な意味

ここでは，われわれが提案したエンタングルメントのエントロピーを実験的もしくは統計的にどう解釈するかを考えてみよう [327]．まずはじめに，相対エントロピーが古典的な情報理論において 2 個の確率分布が与えられたときの区別しやすさの尺度として使われることを示そう．そしてこれを量子の場合に適用し，2 個の量子状態の区別のしやすさの話にする（純粋状態の場合の区別のしやすさについては [328]）．これが量子相対エントロピーに自然に

---

[23] 訳注：現在は加法性の反例が見つかっているため，以下の議論は成り立たない．ただし，$Ed(\rho) \leq E(\rho)$ という結論自身は正しい．しかし，先に述べたように，$E(\rho) \leq Ec(\rho)$ は示されていないので，$Ed(\rho) \neq Ec(\rho)$ は結論できない．

結びつくことを示す．そして，これから，ただちにエンタングルメントの相対エントロピーの概念の説明が得られる．1 個のコインが与えられたときに，コイン投げをして表と裏の出る確率分布が $f = (1/2, 1/2)$ であるかという意味で「公正」であるかどうか検査したいとしよう．もしも偏りがあれば，たとえば $uf = (1/3, 2/3)$ のような確率分布を与えることになる．われわれが考えたいことは有限の n 回のコイン投げの実験をしたとき，どちらの確率分布を与えるかをどれくらい明らかに判明できるかである．n 回コインを投げて表と裏の回数を記録したとき，公正なコインが $(1/3, 2/3)$ の確率分布をもつ不正なコインであると誤認される確率はいくらであろうか？　$f = (1/2, 1/2)$ であるかという意味で「公正」であるかどうか検査したいとしよう．もしも偏りがあれば，たとえば $uf = (1/3, 2/3)$ のような確率分布を与えることになる．結局われわれの問題は，有限の n 回のコイン投げの実験をしたとき，データが二つの確率分布の一方からきているとして，両者をどれだけはっきりと判別できるか，ということに帰着する．n 回コインを投げて表と裏の回数を記録したとき，公正なコインが $(1/3, 2/3)$ の確率分布をもつ不正なコインであると誤認される確率はいくらであろうか？　Stein の補題[24] [327,329] によると，十分に大きい n に対してその答えは

$$p(\text{fair} \to \text{unfair}) \sim e^{-nS_{cl}(uf||f)} \tag{6.52}$$

ただし，$S_{cl} = 1/3 \ln 1/3 + 2/3 \ln 2/3 - 1/3 \ln 1/2 - 2/3 \ln 1/2$ は二つの確率分布に対する古典的な相対エントロピーである．つまり

$$p(\text{fair} \to \text{unfair}) = 3^n 2^{-\frac{5}{3}n} \tag{6.53}$$

となって，$n \to \infty$ に対して等比級数的に 0 に近づく．実際，400 回の試行で誤認の起こる確率は 10^{-10} 程度になる．

Stein の補題の量子版の法則は次のようになる（[327] も参照せよ）．

定理（量子 Stein の補題）n 回の観測で二つの量子状態（密度行列）を区別できない確率 n 回の観測で二つの量子状態（密度行列）を区別できない確率

$$p(\rho \to \sigma) \sim e^{-nS(\sigma||\rho)} \tag{6.54}$$

[24] 訳注：原文では Sanov's theorem. しかし，[329] にもあるように，検定の誤り確率の限界を表すのは Stein の補題で，その証明の鍵になる確率論の定理が Sanov の定理である．以下，Stein の補題と訳しているところは，すべて原文では Sanov's theorem.

である[25].

この値は ρ を観測しながら σ と誤認する確率の下限を示している [327] [26]. 誤認確率は漸近的にこの値に近づくことは示されていて [330], さらにこのような値を実現する射影測定の方法は σ にはよらない [331]. したがって, エンタングルメントの相対エントロピーの解釈は明らかである [327]. もっとも近い非エンタングル状態 ρ をエンタングル状態 σ[27] であると間違う確率は $e^{n\times\min_{\rho\in\mathcal{D}} S(\sigma,\rho)} = e^{-nE(\sigma)}$ となって誤認確率は漸近的にこの値に近づくことは示されていて [330], さらにこのような値を実現する射影測定の方法は σ にはよらない [331]. したがって, エンタングルメントの相対エントロピーの解釈は明らかである [327]. もっとも近い非エンタングル状態 ρ をエンタングル状態 σ であると間違う確率は $e^{n\times\min_{\rho\in\mathcal{D}} S(\sigma,\rho)} = e^{-nE(\sigma)}$ となって[28], σ のエンタングルメントが強くなるに従い, 非エンタングル状態と区別するために必要な測定回数は少なくなる（n を固定して比較すると, 非エンタングルメント状態と間違う確率はより小さくなる）. 例を考えてみよう. 最大限にエンタングルしていると知られている $\sigma := (|00\rangle + |11\rangle)/\sqrt{2}$ を考えてみよう. これに最も近い非エンタングル状態は $\rho := (|00\rangle\langle 00| + |11\rangle\langle 11|)/2$ である [321]. これらを区別するには $(|00\rangle + |11\rangle)/\sqrt{2}$ への射影測定をすればよい. もしも測定対象の状態が ρ であれば, 射影測定の結果は, 射影に成功される回数とそうでない回数はおおよそ半数ずつになるだろう. σ であると誤認されるためにはすべての射影測定の結果が成功となる必要があるので, その確率は 2^{-n} となり, 式 (6.54) で与えられる結果と一致する. もしも測定対象が σ であったとすると, ρ を測定したかのように半々の結果を得ることはありえないので, 式 (6.54) で計算されるように誤認の確率は $e^{-\infty} = 0$ である[29].

---

[25] 訳注：より正確には, $n \to \infty$ で $p(\sigma \to \rho) < \epsilon$ となるという拘束条件のもと, $p(\rho \to \sigma)$ を最適化するのである. すると, $\epsilon > 0$ の値によらず, (6.54) が成立する.

[26] 訳注：[327] にはこのことの証明はなく, 直観的な説明のみがある. だが, こういう直観的説明は以前から専門家には知られていて, たとえば [330] にも説明がある. 厳密な証明は, T. Ogawa and H. Nagaoka *IEEE Trans. Info. Theory*, vol. IT-46, pp. 2428 - 2433 (2000), http://xxx.lanl.gov/abs/quant-ph/9906090. が最初である.

[27] 訳注：原文では ρ.

[28] 訳注：この言明は誤り. 上述の量子 Stein の補題が使えない理由は, 最適な測定が一般には ρ に依存してしまうからである. 前後の文脈から推測するに, 著者らはこの困難を [331] の結果を援用して解決したつもりになっているようだが, そこで述べられているのは, σ に依存しない最適な測定の構成である. おそらく, 引数の順序を誤読したと思われる. また, 最適な測定を p 依存しないようにすることはできない.

[29] 訳注：一般には, Stein の補題の意味で最適な測定では, $\sigma \to \rho$ と誤認する確率のほうが, 逆の誤認確率よりも大きくなるので, この例は非常に特異なケースである.

上記の議論では系の次元やエンタングル状態が2体系であるか多体系であるかには依存しない．これはエンタングルメントを一般的に扱うためにふさわしい性質であり，上記の方法は多体系へ直接拡張できる [322,327]（多体系のエンタングルメント純化処理について述べた8.5節も参照）．

第7章

デコヒーレンスと量子エラー訂正

7.1　はじめに

量子情報処理を実験的に実現する際の主要な障害はデコヒーレンス (decoherence) である．7.2 節においては，量子状態のデコヒーレンスが量子系とその環境とのエンタングルメントによって生じることを示す．7.3 節では，イオントラップ量子コンピュータにおける自然放出によるデコヒーレンスの破壊的影響について説明する．

量子情報分野における最も重要な成果の一つは，デコヒーレンスの問題を克服する方法を発見したことである．この方法は量子エラー訂正 (quantum error correction) 法と呼ばれており，7.4 節で説明する．量子エラー訂正法においては，1 量子ビットの状態を複数量子ビットのエンタングル状態に符号化する．また，エンタングル状態の対称性および量子ノイズは射影測定によってデジタル化できるという事実を利用することによって，量子エラーを検出し訂正する．しかし，エンタングル状態は 1 量子ビット状態よりもデコヒーレンスに弱い．そのため量子エラーを訂正することと発生することの間にトレードオフが存在する．量子エラー訂正の一般論とフォールトトレラント量子計算 (fault-tolerant quantum computation) については 7.5 節で扱う．現実的なエラー訂正法のよい例は，ラムゼイ分光法 (Ramsey spectroscopy) を用いた周波数標準 (frequency standard) の生成の問題である．それについては 7.6 節で説明する．

デコヒーレンスを克服するためのもう一つの方法は，デコヒーレンスによって純粋度 (purity) が減少した多数のエンタングル状態から，純粋度が増した少数のエンタングル状態に蒸留する方法である．このエンタングルメント蒸留 (entanglement distillation) については 8 章で説明する．

7.2　デコヒーレンス

(*A.K.Ekert, G.M.Palma, K.A. Suominen*)

7.2.1　デコヒーレンス：量子ビットと環境とのエンタングルメント

4 章で示したように，量子コンピュータは異なる計算経路が望ましい答えのところで強め合う干渉を行うように設計された一種の「プログラム可能な干渉計」と見なすことができる．そのような干渉を生じさせるためには，計算の時間発展はコヒーレントすなわちユニタリでなければならない．デコヒーレンスによるユニタリ性からのどのようなずれも干渉の可視度 (visibility) を低くしてしまうだろう．

量子ビットが環境と相互作用するときはいつでもデコヒーレンスが生じる．デコヒーレンスの原因を説明するために，量子ビットと環境との相互作用によって，以下の形の結合ユニタリ時間発展が生じると仮定する．

$$|0\rangle\,|E\rangle \xmapsto{U(t)} |0\rangle\,|E_0(t)\rangle \qquad\qquad |1\rangle\,|E\rangle \xmapsto{U(t)} |1\rangle\,|E_1(t)\rangle \tag{7.1}$$

ここで $|E\rangle$ は環境の初期状態，$U(t)$ は結合ユニタリ時間発展演算子である．式 (7.1) を見てわかるように，環境は量子ビットの情報を獲得する測定装置として働く [322]．量子ビットの初期状態が $|0\rangle$ と $|1\rangle$ との重ね合わせ状態のとき，$U(t)$ によって量子ビットと環境との間に次式のようなエンタングルメントが生じる．

$$(a_0\,|0\rangle + a_1\,|1\rangle) \otimes |E\rangle \xmapsto{U(t)} a_0\,|0\rangle\,|E_0(t)\rangle + a_1\,|1\rangle\,|E_1(t)\rangle \tag{7.2}$$

環境の自由度をトレースアウトすると非ユニタリ性が現れる．つまり，デコヒーレンスは式 (7.2) のようなエンタングルメントによって生じるのである．

状態 (7.2) に対応する量子ビットの還元密度行列 (reduced density matrix) は

$$\rho_q(t) = \mathrm{Tr}_E \varrho_{q+E} = \begin{bmatrix} |a_0|^2 & a_0 a_1^* \langle E_1|E_0\rangle \\ a_1 a_0^* \langle E_0|E_1\rangle & |a_1|^2 \end{bmatrix} \tag{7.3}$$

で与えられる．

ほとんどの場合，状態 $|E_0\rangle$ と $|E_1\rangle$ は時間とともにさらに直交するようになる（すなわち量子ビットに関するより多くの情報が環境に漏れるようになる）ので

$$\langle E_0(t)|E_1(t)\rangle = e^{-\Gamma(t)} \tag{7.4}$$

と書くことができる．ここで $\Gamma(t)$ は時間に依存する関数であり，具体的な形は量子ビットー環境間の結合の詳細に依存する [333]．また，その値は量子ビットの種類および環境との相互作用に依存し，10^4 秒（常磁性原子の核スピン）から 10^{-12} 秒（バルク半導体における電子ー正孔励起）まで変化する [334]．結果として，式 (7.2) で表されるエンタングルメントは，占有率 (population) を表す密度行列の対角要素に影響は与えないが，コヒーレンスを表す非対角要素を破壊する．この効果はディフェージング (dephaseing) と呼ばれている．量子ビットー環境のエンタングルメントによって生じる別の効果（散逸）については後で説明する．特徴的なデコヒーレンス時間が量子コンピュータのサイズに対してどのようにスケールされるかを知ることは，計算量理論の観点から重要なことである．それを見るために，式 (7.1) の時間発展を生じる量子ビットー環境の一つの相互作用モデルを導入する．環境系を無限個の調和振動子から構成される熱浴としてモデル化する [333,335]．そして系（1 量子ビットと環境）のハミルトニアンは

$$H = \frac{1}{2}\sigma_z \omega_0 + \sum_{\mathbf{k}} b_{\mathbf{k}}^\dagger b_{\mathbf{k}} \omega_k + \sum_{\mathbf{k}} \sigma_z \left(g_{\mathbf{k}} b_{\mathbf{k}}^\dagger + g_{\mathbf{k}}^* b_{\mathbf{k}} \right) \tag{7.5}$$

で与えられると仮定する．ここで $\omega_{\mathbf{k}}, b_{\mathbf{k}}^\dagger, b_{\mathbf{k}}$ はそれぞれ熱浴のモード $\mathbf{k}$ の周波数，生成演算子，消滅演算子である．また σ_z はパウリ演算子である．右辺第 1 項および第 2 項はそれぞれ量子ビットおよび環境の自由時間発展を記述している．また第 3 項めは量子ビットと環境との相互作用を表している．結合系（量子ビット – 環境）の状態を，密度演算子 $\varrho(t)$ を用いて表す．ここで時

間 $t=0$ における密度演算子を

$$\varrho(0)=|\psi\rangle\langle\psi|\otimes\prod_{\mathbf{k},\mathbf{k}'}|0_{\mathbf{k}}\rangle\langle 0_{\mathbf{k}'}|=\rho(0)\otimes|vac\rangle\langle vac| \tag{7.6}$$

と仮定する．$|\psi\rangle$ は量子ビットの初期状態，$|vac\rangle=\Pi_{\mathbf{k}}|0_{\mathbf{k}}\rangle$ は熱浴の真空状態である．$[\sigma_z,H]=0$ なので，量子ビット系の密度行列 $\rho(t)=\mathrm{Tr}_R\varrho(t)$ の対角項は環境の影響を受けない．しかし量子ビットの量子コヒーレンスは損なわれる．このモデルは厳密に解くことができる．そのため，このモデルを用いることにより，量子ビット－環境のエンタングルメントのメカニズムを明瞭に解析することができる．

相互作用表示における時間発展演算子 $U(t)$ は場に対する条件付変位演算子となり，その変位の符号は量子ビットの論理値に依存することを容易に示すことができる [333]．したがって，$U(t)$ によって式 (7.2) の形のダイナミクスが引き起こされる．このとき

$$\begin{aligned}|E_0\rangle &= \prod_{\mathbf{k}}|-\phi_{\mathbf{k}}\rangle\\ |E_1\rangle &= \prod_{\mathbf{k}}|\phi_{\mathbf{k}}\rangle\end{aligned} \tag{7.7}$$

となる．ここで $|\phi_{\mathbf{k}}\rangle$ は振幅が $\phi_{\mathbf{k}}=g_{\mathbf{k}}\left(1-e^{i\omega_k t}\right)/\omega_k$ のコヒーレント状態である．$\Gamma(t)$ の詳細な計算および有限温度への拡張については文献 [333,335] を参照せよ．

7.2.2　集団的相互作用とスケーリング

以上により，n 量子ビットレジスタのデコヒーレンスを解析する準備ができた．n 量子ビットと環境のハミルトニアンは

$$H=\frac{1}{2}\sum_i\sigma_{z,i}\omega_0+\sum_{\mathbf{k}}b_{\mathbf{k}}^\dagger b_{\mathbf{k}}\omega_k+\sum_{i,\mathbf{k}}\sigma_z\left(g_{i,\mathbf{k}}b_{\mathbf{k}}^\dagger+g_{i,\mathbf{k}}^*b_{\mathbf{k}}\right) \tag{7.8}$$

で与えられる．ここで，結合定数 $g_{i,\mathbf{k}}$ は量子ビットの位置 i に依存する．このハミルトニアンによって

$$\left(\sum_{i_1\cdots i_n}c_{i_1\cdots i_n}|i_1\cdots i_n\rangle\right)\otimes|vac\rangle\overset{U(t)}{\longmapsto}\sum_{i_1\cdots i_n}c_{i_1\cdots i_n}|i_1\cdots i_n\rangle|E_{i_1i_2\cdots i_n}\rangle \tag{7.9}$$

という形のエンタングルメントが引き起こされる．ここで，i_n は n 番めの量子ビットの論理値である．調和振動子から構成される熱浴はコヒーレンス長 λ_c で特徴付けられる．状態 $|E_{i_1 i_2 \cdots i_n}\rangle$ の具体的表式は，レジスタと λ_c のサイズ比に依存した二つの極限の場合に得ることができる．

短い λ_c： この場合，各量子ビットはそれぞれ別々の環境と相互作用する．その結果，独立にデコヒーレンスが生じるので

$$|E_{i_1 i_2 \cdots i_n}\rangle = |E_{i_1}\rangle|E_{i_2}\rangle \cdots |E_{i_n}\rangle \tag{7.10}$$

となる．ここで，$|E_{i_n}\rangle$ は式 (7.7) と同じであり，密度演算子の行列要素は

$$\rho_{i_1 \cdots i_n, j_1 \cdots j_n}(t) = \rho_{i_1 \cdots i_n, j_1 \cdots j_n}(0)\langle E_{i_1}|E_{j_1}\rangle\langle E_{i_2}|E_{j_2}\rangle \cdots \langle E_{i_n}|E_{j_n}\rangle \tag{7.11}$$

のように減衰する．最も速い減衰は

$$\rho_{11\cdots 1,00\cdots 0}(t) = \rho_{11\cdots 1,00\cdots 0}(0)\langle E_1|E_0\rangle^n = \rho_{11\cdots 1,00\cdots 0}(0)e^{-n\Gamma(t)} \tag{7.12}$$

に対して生じる．

長い λ_c： λ_c が十分長いときは，すべての量子ビットは同じ環境と集団的に相互作用すると仮定できる．つまり，すべての量子ビットに対して $g_{i,\mathbf{k}} = g_{\mathbf{k}}$ と仮定できる．このとき，$U(t)$ は全量子ビットの論理値に依存した振幅をもつ条件付変位演算子となる．より具体的には

$$|E_{i_1 \cdots i_n}\rangle = \prod_{\mathbf{k}} \left| -\left\{(-1)^{i_1} + (-1)^{i_2} + \cdots + (-1)^{i_n}\right\} \phi_{\mathbf{k}} \right\rangle \tag{7.13}$$

となる．最も速い減衰は

$$\begin{aligned} \rho_{11\cdots 1,00\cdots 0}(t) &= \rho_{11\cdots 1,00\cdots 0}(0)\langle E_{11\cdots 1}|E_{00\cdots 0}\rangle \\ &= \rho_{11\cdots 1,00\cdots 0}(0)e^{-n^2\Gamma(t)} \end{aligned} \tag{7.14}$$

に対して生じる．指数中の n^2 の物理的起源については，$|E_{00\cdots 0}\rangle$ および $|E_{11\cdots 1}\rangle$ が振幅 $n\phi_{\mathbf{k}}$ のコヒーレント状態のテンソル積であることに注意すれば理解できる．

上の議論により，n 量子ビットレジスタのコヒーレンスの減衰が $\exp[-Poly(n)\gamma(t)]$ [1]のようにスケールされることがわかった．ここで，環境との独立

[1]訳注：$Poly(n)$ とは n の多項式のこと．

な相互作用に対しては $Poly(n) \sim n$ であり，集団的な相互作用に対しては $Poly(n) \sim n^2$ である．

7.2.3　環境と分離した部分空間

前節で見たように，集団的相互作用によってコヒーレンスの減衰はより速くなる．しかし，この集団的相互作用によって環境と分離した部分空間が出現することに注目すべきである．式 (7.13) からわかるように，0 と 1 の数が等しい状態は環境とエンタングルしないのでデコヒーレンスを起こしにくい．別の言い方をすれば，そのような相互作用は場の振幅を変位させない．このことは，環境と分離した部分空間が一種のエラー訂正符号として利用可能であることを示唆している．そこで，$2L$ 量子ビットからなる量子レジスタについて考える．この量子レジスタは互いに十分隣接した量子ビット対から構成されている．そのため各量子ビット対は同じ熱浴と相互作用し，異なる対は異なる熱浴と相互作用すると仮定する．（もしすべての量子ビットが同じ熱浴と相互作用しているとしても結果は同じである．）このとき，論理状態を

$$\begin{aligned} |\tilde{0}\rangle &= |0,1\rangle \\ |\tilde{1}\rangle &= |1,0\rangle \end{aligned} \tag{7.15}$$

と符号化する．つまり，1 量子ビットを一対の量子ビットに符号化すれば，レジスタを環境から効果的に分離できるであろう．

しかし，この種の符号化に関していくつかの問題が未解決のままである．まず第 1 に，そのような状態が別の種類のデコヒーレンスに対しても強固であることを確かめるべきである（この疑問については次節で議論する）．次に，（環境と分離した状態は外部プローブとも結合しないので）そのような状態をどのようにして準備し，どのようにして読み出すのかという問題（これは一括測定をすることを意味する）も残されている．最後に，そのような部分空間の中でどのように量子計算を行うのかについてもはっきりとした答えはない．量子ビット間の制御可能な相互作用は，ゲート演算の実装に対して役立つであろう [336,337]．

7.2.4　他の種類の結合

この節の残りで，量子ビットと環境の相互作用に対するより現実的なメカニズムについて考察する．そして，いままで得られた結果の中で，どの方法

が生き残るかについて調べる．解析に用いるモデルは，量子光学における電磁場と 2 準位原子間の光子交換のような幅広い範囲の物理現象の記述に用いられるものである．この調和振動子熱浴と結合した n 個の同一量子ビットからなるモデルのハミルトニアンは

$$H = \frac{1}{2}\sum_i \sigma_{z,i}\omega_0 + \sum_{\mathbf{k}} b_{\mathbf{k}}^\dagger b_{\mathbf{k}}\omega_{\mathbf{k}} + \sum_{i,\mathbf{k}} \left(g_{i,\mathbf{k}}\sigma_{-,i}b_{\mathbf{k}}^\dagger + g_{i,\mathbf{k}}^*\sigma_{+,i}b_{\mathbf{k}}\right) \tag{7.16}$$

で与えられる．ここで，$\sigma_{-,i}$ および $\sigma_{+,i}$ はそれぞれ量子ビット i の下降および上昇演算子である．

式 (7.16) によって生成されるダイナミクスは厳密に解くことはできない．しかし，ボルン－マルコフ近似のもとでは，量子ビットの還元密度行列の時間発展はマスター方程式によって記述できる [338,339]．量子ビット間の距離が共鳴モードの波長よりも短ければ，$g_{i,\mathbf{k}} \sim g_0$ と近似でき，マスター方程式は

$$\frac{d\rho}{dt} = i\omega_0\rho - \frac{\gamma}{2}\left(S_+S_-\rho + \rho S_+S_- - 2S_-\rho S_+\right) \tag{7.17}$$

で与えられる．ここで，集団的演算子 $S_\pm = \sum_i \sigma_{\pm,i}$ と減衰定数 $\gamma \propto |g_0|^2\,\delta(\omega_{\mathbf{k}} - \omega_0)$ を導入した．

式 (7.17) によって記述されるダイナミクスは明らかに非ユニタリである．前節の厳密に解けるモデルに比べてあまり自明ではないが，非ユニタリ性は量子ビットと環境とのエンタングルメントにより生じる．

1 量子ビットの場合，時刻 t での還元密度演算子は

$$\rho(t) = \begin{pmatrix} (1-\rho_{11})\,e^{-\gamma t} & \rho_{10}e^{-\frac{\gamma}{2}t} \\ \rho_{01}e^{-\frac{\gamma}{2}t} & \rho_{11}e^{-\gamma t} \end{pmatrix} \tag{7.18}$$

となり，デコヒーレンスと同時に占有率の減衰（散逸）が引き起こされる．

このモデルにおける集団的相互作用の性質を説明するために，ベル状態 $|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ の減衰について見てみよう．状態 $|00\rangle$ への減衰に対する確率振幅は，演算子 S_+ の行列要素

$$\langle\Psi_\pm|S_+|00\rangle = \frac{1}{\sqrt{2}}\left(\langle 01|\sigma_{+2}|00\rangle \pm \langle 10|\sigma_{+1}|00\rangle\right) \tag{7.19}$$

に比例する．状態 $|\Psi_+\rangle$ の場合，確率振幅 (amplitude) は強め合う干渉を行う．その結果，減衰率は 1 量子ビットの場合の 2 倍になる．したがって量子ビッ

ト数 n が大きいとき，集団的減衰のために減衰定数のスケーリングは $n\gamma$ から $n^2\gamma$ へ変化する．一方状態 $|\Psi_-\rangle$ の場合，確率振幅は打ち消し合う干渉を行う．そのため，状態 $|\Psi_-\rangle$ は環境系と結合しなくなる．これは，超放射対抑制放射 (superradiance v.s. subradiance) として知られる現象である．またこれにより，n 量子ビットのレジスタとして抑制放射部分空間を用いることが可能であると考えられる [341]．もちろんこの場合においても，前節で述べたすべての未解決問題が残されている．

以上をまとめると，異なるモデルを用いると異なる減衰機構が生じ，それらの取り扱いには異なる手法が必要になることがわかった．しかし，デコヒーレンス過程の定性的性質のほとんどはモデルに依存しない．特に，すべてのデコヒーレンス過程は量子レジスタの非ユニタリ時間発展を引き起こすであろう．さらに集団的相互作用はある部分空間の減衰を強めるが，他の部分空間の減衰を抑制する．したがって，前節における量子コンピュータのサイズに対するデコヒーレンス時間のスケーリングおよび集団的符号化に対する考察は，環境との結合の詳細にかかわらず有効である．

7.3　デコヒーレンスによる量子計算の限界

(*M.B. Pleino, P.L. Knight*)

前節において，イオン列（5 章）のような量子ビット列に生じるデコヒーレンスと散逸を記述するモデルを示した．この節においては，量子コンピュータにおいてノイズの影響がどの程度重大であるかについて定量的に考察する．特に，イオントラップ量子コンピュータ [156]（動作原理については 4.3 節と 5 章を見よ）において何ステップの量子演算が可能かについて調べる．ここでは，核磁気共鳴 (NMR) 方式 [342,343]（5.4 節）のような他の種類の量子コンピュータについては議論しない．

量子コンピュータにおいては，ノイズを発生するメカニズムが多数存在する．しかし，この節においてはイオンからの自然放出による影響 [344-347] についてのみ議論する．なぜならば，解析がかなり簡単であるからである．重心モードにおけるノイズ [348]，レーザ不安定性，異なるイオン間のクロストーク [349] のような他のメカニズムについてはここでは議論しない．これらの効

果については参考文献を見よ．

さて，量子コンピュータにおける自然放出の影響について考察しよう．そのための基準として素因数分解アルゴリズム [350] を用いる．以下の議論は他のアルゴリズムに対しても簡単に一般化できる．4.2 節で示したように，古典コンピュータを用いて大きな整数を素因数分解するのは難しい問題であり，効率的には実行できない．しかし，量子コンピュータを用いた効率的なアルゴリズムが発見された．理想的な条件下では，量子コンピュータを用いれば古典コンピュータよりも指数関数的に高速に素因数を見つけることができる．そこで，エラーの原因がイオンからの自然放出だけであると仮定した場合に，量子コンピュータを用いて素因数分解可能な最大の整数を求める．解析を簡単化するために，ここでは量子エラー訂正の実現性については考えない．これについては，文献 [346] および次節を見よ．

以下のような実験構成について考える．イオン列が線形イオントラップ中に置かれており，運動の基底状態に冷却されている．各量子ビットはイオン内の準安定光学遷移によって表現される．考察しているイオンの内部構造を図 7.1 に示す．量子ビットは原子準位 0 と 1 によって表現される．状態間の遷移はラビ周波数 Ω_{0i} をもつレーザにより駆動され，準位 i からの自然放出は割合 $2\Gamma_{ii}$ で生じる．付加的準位 2 の存在は重要であり，それについては後で議論する．もちろん，ゼーマン副準位 (Zeeman sublevel) のようなより精巧な量子ビットの表現法も存在する．しかし，話がより複雑になってしまうだけで結論は変わらない．詳細については文献 [346] を見よ．

われわれの目的は，L ビットの整数を素因数分解することである．つまり，整数の値は 2^L より小さい．Shor のアルゴリズムを用いれば，この計算は ϵL^3 回の基本量子演算（1 量子ビットゲート，CNOT ゲート，トフォリゲートなど）を用いて実行できる．この計算を実行する量子ネットワークは文献 [351] において設計され，L ビットの整数を素因数分解するために $5L$ のオーダの量子ビットが必要であることがわかっている．

必要なゲートをすべて実行するのにどれくらいの時間を要するのであろうか．1 個のトフォリゲートを実行するために必要な時間は，1 個の CNOT ゲートの実行時間の 1.5 倍である [156]．したがって，CNOT ゲートを実行するのに必要な時間を計算するだけで十分である．1 量子ビットゲートはより高速に実行できるので，それについては考えない．1 量子ビットゲートが高速な

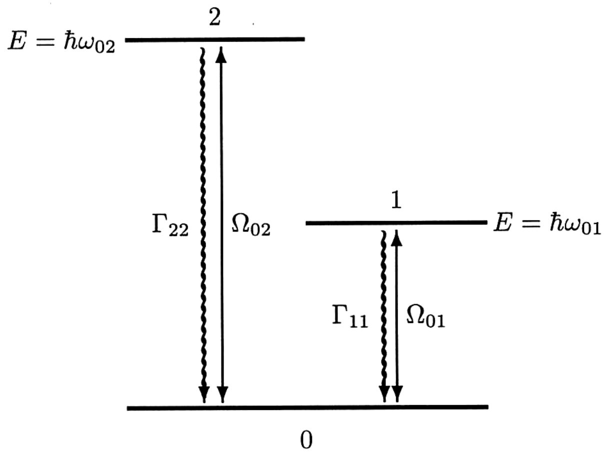


図 7.1　量子計算に用いられるイオンの準位の概略図．$0 \leftrightarrow 1$ 遷移は量子ビットを表す．量子ビットは，ラビ周波数 Ω_{01} のレーザにより駆動される．準位 1 の自然放出率は $2\Gamma_{11}$ であり，小さいと仮定する．$0 \leftrightarrow 1$ 遷移と共鳴するレーザにより，準位 0 と準位 2 のようなその他の非共鳴準位との結合が生じてしまう．$0 \leftrightarrow 2$ 遷移のラビ周波数は Ω_{02} であり，減衰率 $2\Gamma_{22}$ は普通は $2\Gamma_{11}$ よりもかなり大きい．レーザは $\Delta_{02} \gg \Omega_{02}$ だけ $0 \leftrightarrow 2$ 遷移から離調しているので，$0 \leftrightarrow 2$ 遷移の有効ラビ周波数は大変小さい

理由は，CNOT ゲートと異なり重心モードの励起を必要としないからである（5.2.9 項を見よ）．

CNOT ゲートの実行に要する時間は

$$\tau_{el} = 4\pi \frac{\sqrt{5L}}{\eta\Omega_{01}} \tag{7.20}$$

である．ここで，$5L$ はトラップ中のイオン数，Ω_{01} は量子ビット遷移を駆動するレーザのラビ振動数，η はラムーディッケ・パラメータである（実験の詳細については 5 章を見よ）．したがって，L ビットの整数を素因数分解するのに要する時間は CNOT ゲート数に τ_{el} を掛けたものであり

$$T = \frac{4\pi\sqrt{5L}}{\eta\Omega_{01}} \epsilon L^3 \tag{7.21}$$

となる．この表式の中に明らかに自由に制御できるパラメータがある．たとえば，速い計算を行うためにラビ周波数 Ω_{01} を増加させる場合について考え

てみる．これによって，量子ビットの上準位からの自然放出を避けることができるであろう．しかし，これはそんなに簡単なことではない．なぜならば，遷移のラビ周波数 Ω とその遷移の減衰定数 Γ は互いに

$$\frac{\Omega^2}{\Gamma} = \frac{6\pi c^3 \epsilon_0}{\hbar\omega_{01}^3} E^2 \tag{7.22}$$

によって関連しているからである．ここで，E はレーザの電場強度，c は光速，ϵ_0 は真空誘電率，ω_{01} は遷移周波数である．それでは，レーザの電場強度 E を増加してもよいのではと考えられないだろうか．明らかに，このプロセスにはある上限が存在する．もし E が電子と原子核の間の電場強度を越えるほど強ければイオンはすぐに電離するであろう．しかし，これはかなり高い値なので他の効果のほうがより顕著になる．実際電場強度が強い場合，イオンを 2 準位系であると仮定することはできない．なぜならば，他のエネルギー準位が非共鳴遷移によりわずかに占有され，それらの準位がダイナミクスに寄与するようになるからである．この状況を図 7.1 に示す．量子ビット準位 0 と 1 に加えて，他の離調した準位が存在する．すべての離調準位の影響を準位 0 と結合する一つの補助準位 2 としてまとめて表す．レーザは，$0 \leftrightarrow 2$ 遷移の共鳴から大きくずれているので，準位 2 の占有率は小さいであろう．にもかかわらず，この補助準位 2 は大変短い寿命をもつので，準位 2 からの自然放出が起こるであろう．レーザ強度を強くすればするほど，補助準位の占有率が大きくなる．したがって，量子ビット準位 1 からの自然放出と補助準位 2 からの自然放出の間にトレードオフが存在する．つまり，計算を速くすればするほど，量子ビット準位 1 からの自然放出は減るが，補助準位 2 からの自然放出が増加してしまう．

以下，準位 1 および準位 2 からの自然放出確率 p_{tot} を計算する．その目的は，この確率を最小化することである．この最小化により，(自然放出が存在するとき) 量子コンピュータによって素因数分解可能な整数の大きさの上限が得られる．

すべての量子計算の間に，平均として量子ビットの半分が準位 1 にある．したがって，その間に準位 1 から自然放出する確率は

$$p_1 = \frac{1}{2} 2\Gamma_{11} 5LT \tag{7.23}$$

で与えられる．一方，補助準位 2 はイオンがレーザと相互作用している間だ

け占有される．したがって，補助準位 2 が自然放出する確率は

$$p_2 = \frac{\Omega_{02}^2}{8\Delta_{02}} 2\Gamma_{22} T \tag{7.24}$$

で与えられる．次に式 (7.22) を用いると

$$\frac{\Omega_{01}^2}{\Gamma_{11}} = \frac{\omega_{02}^3}{\omega_{01}^3} \frac{\Omega_{02}^2}{\Gamma_{22}} \tag{7.25}$$

が得られる．また

$$x = \sqrt{\frac{\Omega_{01}^2}{\Gamma_{11}}} \tag{7.26}$$

と定義すると，式 (7.21) を用いることにより

$$\begin{aligned} p_{tot} &= p_1 + p_2 & (7.27) \\ &= \frac{4\pi\sqrt{5L}}{\eta} \epsilon L^4 \sqrt{\Gamma_{11}} \left(\frac{1}{x} + \frac{1}{L} \frac{\omega_{01}^3}{\omega_{02}^3} \frac{\Gamma_{22}^2}{\Delta_{02}^2 \Gamma_{11}} x \right) & (7.28) \end{aligned}$$

を得る．この式を x に関して最小化することにより，最小値

$$p_{min} = \frac{4\pi\sqrt{5}\epsilon L^4}{\eta} \sqrt{\frac{\omega_{01}^3}{\omega_{02}^3}} \sqrt{\frac{\Gamma_{22}^2}{\Delta_{02}^2}} \tag{7.29}$$

を得る．量子計算を行っている間，自然放出が起こらないことを高い確率で保証するためには，$p_{min} \ll 1$ であればよい．したがって，式 (7.29) を L の上限

$$L_{max}^8 \approx \frac{\eta^2 \Delta_{02}^2}{80\Gamma_{22}^2 \pi^2 \epsilon^2} \left(\frac{\omega_{02}}{\omega_{01}} \right)^3 \tag{7.30}$$

に変形することができる．式 (7.30) において L^8 のべきはどこから生じたのであろうか．その理由は，図 7.2 に示した正のフィードバックループである．

これが重大な制限であるのかどうかを調べるために，この式の中に具体的な値を代入する必要がある．ここでは現実のイオン，すなわちイオントラップ実験で用いられている値を用いる．

表 7.1（文献 [346] からの抜粋）において，いくつかの現実の原子に対する結果を示す．素因数分解可能な整数の上限は非常に小さい．このことは，自

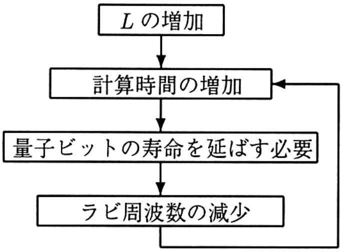


図 7.2 正のフィードバックのために式 (7.30) において強い L 依存性が表れる．L を大きくすると計算時間が長くなる．そのために，量子ビットの寿命を長くする必要がある．それは，量子ビット遷移における達成可能なラビ周波数を減少させてしまう．これにより計算時間がさらに長くなってしまう

然放出によるノイズですら量子計算に重大な制限を与えることを示している．このため，この分野の研究者は自然放出のようなノイズによって引き起こされたエラーを訂正する方法を開発しているのである．この方法については次節で説明する．実際この方法により，この節で導いた上限を改善することができる．

7.4 量子エラー訂正とフォールトトレラント量子計算

(*C. Macchiavello, G.M. Palma*)

7.4.1 対称化法

量子コンピュータに生じた量子ノイズに対して最初に提案された対処法は，対称化法 (symmetrization procedure)[352] である．この節では対称化法の基本概念について簡単に述べる．量子系をある初期状態 $|\Psi_i\rangle$ に用意し，ある指定されたユニタリ発展 $|\Psi(t)\rangle$ を行いたい，あるいは $|\Psi_i\rangle$ をある時間 t の間保存したいと仮定する．また，単一系の代わりに $|\Psi_i\rangle$ のコピーを R 個用意でき，その後結合系の状態を対称部分空間（部分系の任意の置換に対し不変である状態すべてを要素とする部分空間）に射影できると仮定する．状態を対称部分空間に頻繁に射影することで，環境によって引き起こされたエラーを

表 7.1　量子コンピュータを用いて素因数分解可能な整数 N のビット数 L の上限．量子ビットは準安定光学遷移により表現される．図 7.1 中の準位 0，1，2 の状態も示す．データを式 (7.30) に代入することにより L の上限（表の最終行）を計算した

イオン	Ca^+	Hg^+	Ba^+
準位 0	$4s\ ^2S_{1/2}$	$5d^{10}\ 6s^2\ ^2S_{1/2}$	$6s\ ^2S_{1/2}$
準位 1	$3d\ ^2D_{5/2}$	$5d^9\ 6s^2\ ^2D_{5/2}$	$5d\ ^2D_{5/2}$
準位 2	$4s\ ^2P_{3/2}$	$5d^{10}\ 6p^2\ ^2P_{1/2}$	$6s\ ^2P_{3/2}$
$\omega_{01}[s^{-1}]$	$2.61 \cdot 10^{15}$	$6.7 \cdot 10^{15}$	$1.07 \cdot 10^{15}$
$\omega_{02}[s^{-1}]$	$4.76 \cdot 10^{15}$	$11.4 \cdot 10^{15}$	$4.14 \cdot 10^{15}$
$\Gamma_{22}[s^{-1}]$	$67.5 \cdot 10^6$	$5.26 \cdot 10^8$	$58.8 \cdot 10^6$
$L(\eta = 0.01)$	2.2	1.6	4.5

減らせるというのがこの方法の主張していることである．この発想は，対称部分空間から時間発展を始めた R 個の独立なコピーの状態は，その後もその部分空間にとどまるはずであるという事実に基づいている．したがって，エラーを起こしていない構成要素は，常に対称部分空間の中に存在するので，射影しても状態は不変である．一方，エラーを含む構成要素は取り除かれる．しかしながら，対称部分空間は単純な直積の形 $|\Psi\rangle|\Psi\rangle\cdots|\Psi\rangle$ では表せない状態を含む．そのため，射影された状態は一般にエラーを起こしていない状態ではないことに注意せよ．にもかかわらず，エラー確率は $1/R$ に抑制される [353]．

ここで，2 量子ビットの最も簡単な場合について説明する．この場合，対称部分空間への射影は対称化演算子

$$S = \frac{1}{2}\left(P_{12} + P_{21}\right) \tag{7.31}$$

によって行われる．ここで P_{12} は単位行列，P_{21} は二つの量子ビット状態を交換する置換演算子である．2 量子ビットの純粋状態 $|\Psi\rangle$ を対称化部分空間へ射影した状態は $S|\Psi\rangle$ となる．このとき，この状態を再規格化する必要がある．2 量子ビットの混合状態に対する写像は（規格化を含めて）

$$\rho_1 \otimes \rho_2 \longrightarrow \frac{S\left(\rho_1 \otimes \rho_2\right) S^\dagger}{\mathrm{Tr} S\left(\rho_1 \otimes \rho_2\right) S^\dagger} \tag{7.32}$$

で与えられる．各量子ビットの状態は，別の量子ビットに関して部分トレースをとることにより得られる．

ある純粋状態 $\rho_0 = |\Psi\rangle\langle\Psi|$ の二つのコピーを最初に用意し，それぞれが独立な環境と相互作用すると仮定する．ある時間 δt の後に，二つのコピーの状態 $\rho^{(2)}$ は

$$\rho^{(2)}(0) = \rho_0 \otimes \rho_0 \longrightarrow \rho^{(2)}(\delta t) = \rho_1 \otimes \rho_2 \tag{7.33}$$

のように時間発展するであろう．ここで $\rho_i = \rho_0 + \varrho_i$ であり，e_i は零トレースのエルミート演算子である．ϱ_i の 1 次の項まで考慮すると，時間 δt 後の全系の状態は

$$\rho^{(2)} = \rho_0 \otimes \rho_0 + \varrho_1 \otimes \rho_0 + \rho_0 \otimes \varrho_2 + O(\varrho_1 \varrho_2) \tag{7.34}$$

となる．

2 乗した密度演算子の平均トレース

$$\frac{1}{2}\sum_{i=1}^{2} \mathrm{Tr}\left((\rho_0 + \varrho_i)^2\right) = 1 + 2\mathrm{Tr}(\rho_0 \tilde{\varrho}) \tag{7.35}$$

($\tilde{\varrho} = \frac{1}{2}(\varrho_1 + \varrho_2)$) から，対称化後の二つのコピーの平均純粋度が得られる．$\mathrm{Tr}(\rho_0 \tilde{\varrho})$ は負なので，式 (7.35) は 1 を超えない．対称化後の各量子ビットの状態は

$$\rho_s = [1 - \mathrm{Tr}(\rho_0 \tilde{\varrho})]\, \rho_0 + \frac{1}{2}\tilde{\varrho} + \frac{1}{2}\left(\rho_0 \tilde{\varrho} + \tilde{\varrho}\rho_0\right) \tag{7.36}$$

となり，純粋度は

$$\mathrm{Tr}(\rho_s^2) = 1 + \mathrm{Tr}(\rho_0 \tilde{\varrho}) \tag{7.37}$$

となる．$\mathrm{Tr}\rho_s^2$ は式 (7.35) よりも 1 に近い．したがって，対称化された系 ρ_s は，対称化前の状態に比べてより純粋な状態になる．

次に，対称化法の適用による忠実度 (fidelity) の変化について調べる．対称化前の平均忠実度は

$$F_{bs} = \frac{1}{2}\sum_{i} \langle\Psi|(\rho_0 + \varrho_i)|\Psi\rangle = 1 + \langle\Psi|\tilde{\varrho}|\Psi\rangle \tag{7.38}$$

である．一方，対称化後は

$$F_{bs} = \langle\Psi|\rho_s|\Psi\rangle = 1 + \frac{1}{2}\langle\Psi|\tilde{\varrho}|\Psi\rangle \tag{7.39}$$

となる．したがって，対称化後の状態のほうがより初期状態 ρ_0 に近い．

コピーが R 個の一般的な場合，対称化後の各量子ビットの純粋度は

$$\mathrm{Tr}(\rho_s^2) = 1 + 2\frac{1}{R}\mathrm{Tr}(\rho_0\tilde{\varrho}) \tag{7.40}$$

で与えられる [353]．ここで $\tilde{\varrho} = \frac{1}{R}\sum_{i=1}^{R}\varrho_i$ である．このとき忠実度は

$$\langle\Psi|\rho_s|\Psi\rangle = 1 + \frac{1}{R}\mathrm{Tr}(\rho_0\tilde{\varrho}) \tag{7.41}$$

となる．

式 (7.40) と (7.41) は，それぞれ対応する対称化前の状態 (7.35) と (7.38) と比較する必要がある．R が無限大に向かうと ρ_s は無摂動状態 ρ_0 近づくことがわかる．したがって，R を十分大きく選び，また対称化射影を頻繁に行えば，計算終了後に残るエラーを原理的に任意の微小許容範囲内に抑制することができる．

7.4.2　古典エラー訂正

別の種類の量子エラー訂正法が，古典エラー訂正符号 [354] を量子系に拡張することによって得られる．実際，エラーが存在するときに情報を確実に伝送し操作するという問題は，古典情報理論の中で扱われてきた．そこで，量子エラー訂正符号 (quantum error correcting code) の解析を始める前に，古典エラー訂正について簡単に復習する．以下，c 個の符号語（長さ n の 2 進系列）の集合 $\mathbf{w}_1 \cdots \mathbf{w}_c$ のことを符号 (code) と定義する．情報の伝送あるいは保存の間に，ノイズの影響でいくつかのビットがランダムに反転する．このビット反転が唯一の古典エラーである．

もし通信路が図 7.3 のような 2 元対称無記憶通信路 (binary symmetric memoryless channel)[2]であれば，受信系列 $\mathbf{v}_1 \cdots \mathbf{v}_{2^n}$ は，長さ n のすべての 2 元系列の集合（元の数は 2^n 個）になる．受信者は，ある受信系列 $\mathbf{v}_0$ に最も近い送

[2]訳注：通信路が「対称」であるとは，0 から 1 へ反転する確率と 1 から 0 へ反転する確率が等しいということ．また，通信路が「無記憶」であるとは，通信路を使用するごとに同じ確率分布でビットが変化し，かつそれは使うごとに独立であるということ．

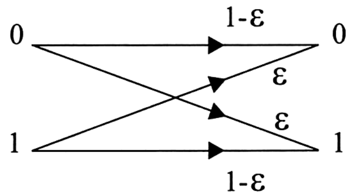


図 **7.3**　2 元対称通信路においては，各ビットはエラー確率 ϵ で伝送される

信語 $\mathbf{w}_i$ を探す．二つの 2 元系列間の距離 $d(\mathbf{w}, \mathbf{v})$ はハミング距離 (Hamming distance) と呼ばれ，二つの系列の中で異なるビット数として定義される[3]．2 元対称無記憶通信路の場合，$\mathbf{w}_i$ として最小ハミング距離 $d(\mathbf{w}_i, \mathbf{v}_0)$ のものが選ばれる．

符号語間の距離を長くすればするほど，それらの符号語はエラーが存在するときによりはっきりと区別できるようになる．したがって，その符号はよりノイズに対して強くなる．もし，$i \neq j$ に対して $d(\mathbf{w}_i, \mathbf{w}_j) \geq 2\eta + 1$ であれば，η 個以内のエラーを訂正することができる．

ハミング限界 (Hamming bound) は，η 個までのエラーを訂正するために必要な符号語数 c の上限を与える．各符号語は半径 η の球[4]の中心に位置する．また，その球の中には $d(\mathbf{w}_i, \mathbf{v}) \leq \eta$ を満足するすべての 2 元系列が含まれる．つまり，$\mathbf{w}_i$ から η 個以内のビットを反転した系列すべてが含まれる．図 7.4 に $\eta = 4$ の場合の例を示す．この符号がエラー訂正可能であるためには，これらの球は重なってはいけない．さらに，それぞれの球中の系列数に球の全数を掛けたものは，長さ n の系列の総数よりも小さくなくてはいけない．それぞれの球の中には，一つの符号語 $\mathbf{w}$ とそれから $1, 2, \cdots, \eta$ 個のビットが異なる系列すべてが含まれる．したがって，ハミング限界

$$c\left\{1 + n + \binom{n}{2} + \cdots + \binom{n}{\eta}\right\} = c\sum_{i=0}^{\eta}\binom{n}{i} \leq 2^n \tag{7.42}$$

が得られる．

効率的な符号の一つとして，パリティ検査符号 (parity check code)[354] が知られている．この符号の符号語 $\mathbf{w}$ は，ある線形方程式の集合を満足するよ

[3]訳注：たとえば，$d(0000, 0101) = 2$ である．
[4]訳注：ハミング球 (Hamming sphere) と呼ばれる．

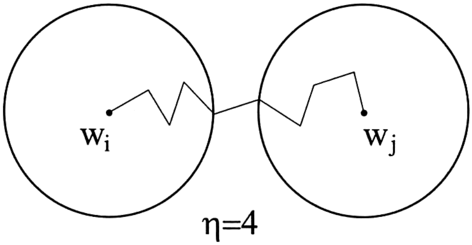


図 7.4　$d(\mathbf{w}_i, \mathbf{w}_j) \geq 2\eta + 1$ である符号において，各符号語を中心とした半径 η の球の中には，η 個までのエラーを起こした系列すべてが含まれる

うに選ばれる．受信者は受信した系列 $\mathbf{v}$ がこの方程式の集合を満足するかどうかをテストする．もし，$\mathbf{v}$ が方程式を満足しなければ，受信者はエラーを訂正する．符号語が満足すべき方程式の集合[5]は，パリティ検査行列 (parity check matrix)$\mathbf{M}$ に対応付けられる．つまり，符号語 $\mathbf{w}$ は関係式

$$\mathbf{M} \cdot \mathbf{w} = 0 \tag{7.43}$$

を満足するように選ばれる．たとえば，符号語

$$\mathbf{w}_1 = 0000 \qquad \mathbf{w}_2 = 0101 \qquad \mathbf{w}_3 = 1110 \qquad \mathbf{w}_4 = 1011 \tag{7.44}$$

はパリティ検査行列が

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \tag{7.45}$$

の場合の方程式 (7.43) を満足する．ここで，和に関しては mod 2 の演算を行う．$\mathbf{M}$ の階数が m のとき，符号語の中の $k = n - m$ ビットは情報ビットを表す．一方，残りの m ビットは検査ビットであり，式 (7.43) から決定される．したがって，線形独立な符号語の数は $c = 2^{n-m} = 2^k$ となる．このときハミング限界の式 (7.42) は

$$2^k \sum_{i=0}^{\eta} \begin{pmatrix} n \\ i \end{pmatrix} \leq 2^n \longrightarrow 2^{n-k} = 2^m \geq \sum_{i=0}^{\eta} \begin{pmatrix} n \\ i \end{pmatrix} \tag{7.46}$$

[5]訳注：パリティ検査方程式 (parity check equation) と呼ばれる．

となる．この式は，検査ビット数 $m = n - k$ の下限を与える．系列 $\mathbf{w}$ を伝送し，系列 $\mathbf{v}$ が受信されたとする．このとき，系列 $\mathbf{z} = \mathbf{w} - \mathbf{v}$ はエラーが生じたビットは 1 となりその他は 0 となる 2 元系列であり，エラーパターン (error pattern) と呼ばれる．もし $\mathbf{z} \neq 0$ であれば，$\mathbf{v}$ は検査方程式を満足しない．つまり，$\mathbf{M} \cdot \mathbf{v} = \mathbf{M} \cdot (\mathbf{w} + \mathbf{z}) = \mathbf{M} \cdot \mathbf{z} = \mathbf{s}$ となる．ベクトル $\mathbf{s}$ はエラーシンドローム (error syndrome) と呼ばれ，$\mathbf{Z}$ が 1 となる位置に対応する $\mathbf{M}$ の列を足したものである．たとえば，$\mathbf{w} = 1110$ が伝送され $\mathbf{v} = 1000$ が受信されたとする．このとき $\mathbf{z} = 0110$ であり，$\mathbf{s} = 10$ となる．

受信者はエラーシンドローム $\mathbf{s}$ からエラーパターン $\mathbf{z}$ を同定し，エラーを訂正する．単一エラーを訂正可能な符号のシンドロームは，エラーが生じたビットを j とすると，対応するパリティ検査行列 $\mathbf{M}$ の j 列めである．もし $\mathbf{M}$ の各列が互いに異なっていれば，受信者は容易にエラーの位置を同定し，それを訂正することができる．

7.4.3 量子エラー訂正符号の一般的側面

古典エラー訂正法を量子系に拡張しようとすると次の問題に直面する．

1. 外部ノイズによって量子ビットの論理値が反転するだけではなく，デコヒーレンスも生じる．また 7.2 節で見たように，一般に量子ビット系は環境とエンタングルしてしまう．
2. 量子計算が終了する前に量子ビットの状態を読み出してはいけない．読み出しを行うと状態が壊れてしまう．したがって，量子ビットの状態に関する情報を獲得すること無しにエラーの位置と性質に関する情報を獲得しなければならない．

以下，**符号ベクトル** (code vector)$|\mathbf{w}\rangle$ として n 量子ビットのエンタングル状態を用いることにより 2 番めの問題が回避できることを示す．したがって，われわれが保護したい情報は，n 量子ビットすべてがエンタングルした状態に広がる．量子ビットの観測（あるいはデコヒーレンス）によって必ずしも不可逆的に量子情報が失われるわけではない．符号ベクトル $|\mathbf{w}\rangle$ としては，エラーが生じると $|\mathbf{w}\rangle$ が互いに直交する部分空間に移るようなものが選ばれる．シンドロームの測定により，どの部分空間に $|\mathbf{w}\rangle$ が移ったのかに関する情報だけが明らかになる．以下，それぞれの量子ビットのエラー確率を ϵ と

し，異なる量子ビットのエラーは互いに独立に生じると仮定する．このため，二つの量子ビットにエラーが生じる確率は $O(\epsilon^2)$ である．ϵ が十分小さいときは，1 量子ビットのエラーしか生じないと仮定できる．このとき，計算が成功する確率は $(1-\epsilon)$ である．もし，単一エラーを訂正可能な量子エラー訂正符号を用いれば，成功確率は $(1-O(\epsilon^2))$ となる．一般に，t 個までのエラーを訂正可能な符号を用いた場合，成功確率は $(1-O(\epsilon^{t+1}))$ と増加する．

7.4.4　3 量子ビット符号

量子エラー訂正符号に親しんでもらい，また上で概説したアイデアを説明するために，3 量子ビット符号について解析を行う．この符号を用いることにより，1 量子ビットの位相エラーを訂正することが可能となる [355]．符号語を構成する各量子ビットは，環境と独立に式 (7.1) のようにエンタングルすると仮定する．以下，位相エラー

$$|0\rangle \longrightarrow |0\rangle \qquad\qquad |1\rangle \longrightarrow -|1\rangle \tag{7.47}$$

を訂正できれば，位相エンタングルメントの影響を元に戻すことができることを示す．位相エラーはエラー演算子 σ_z によって表される．このようなエラーを訂正するために，符号語として次のような 3 量子ビットのエンタングル状態を用いる．

$$\begin{aligned} |\mathbf{w}_0\rangle &= |000\rangle + |011\rangle + |101\rangle + |110\rangle \\ |\mathbf{w}_1\rangle &= |111\rangle + |100\rangle + |010\rangle + |001\rangle \end{aligned} \tag{7.48}$$

もし，1 個の量子ビットだけが環境とエンタングルすれば，任意の $|\mathbf{w}_0\rangle$ および $|\mathbf{w}_1\rangle$ の重ね合わせ状態は

$$\begin{aligned} (a_0|\mathbf{w}_0\rangle + a_1|\mathbf{w}_1\rangle)\,|E\rangle \longrightarrow\ & (a_0|\mathbf{w}_0\rangle_0 + a_1|\mathbf{w}_1\rangle_0)\,|E_0\rangle \\ +\ & (a_0|\mathbf{w}_0\rangle_1 + a_1|\mathbf{w}_1\rangle_1)\,|E_1\rangle \\ +\ & (a_0|\mathbf{w}_0\rangle_2 + a_1|\mathbf{w}_1\rangle_2)\,|E_2\rangle \\ +\ & (a_0|\mathbf{w}_0\rangle_3 + a_1|\mathbf{w}_1\rangle_3)\,|E_3\rangle \end{aligned} \tag{7.49}$$

となる．ここで，エラー状態 $|\mathbf{w}_j\rangle_k$ は，符号語 $j(=0,1)$ の k 番めの量子ビットに位相エラーが生じた状態である（$k=0$ はエラーなしに対応）．たとえ

ば，$|\mathbf{w}_0\rangle_2 = |000\rangle - |011\rangle + |101\rangle - |110\rangle$ である．また，$|E_k\rangle$ は対応する環境の状態である．エラー状態は互いに直交することに注意せよ．

$$ {}_k\langle \mathbf{w}_j | \mathbf{w}_l \rangle_i = \delta_{jl}\delta_{ki} \tag{7.50} $$

エラー状態が直交するような符号は，非縮退 (non-degenerate) 符号と呼ばれる．したがって，エラー訂正は以下のように行う．

- 状態を $|\mathbf{w}_0\rangle_i$ および $|\mathbf{w}_1\rangle_i$ によって張られるエラー部分空間に射影する．
- 測定結果から，位相エラーがどの量子ビットに生じたかがわかる．そこで，その量子ビットに σ_z を作用することによって位相エラーを訂正する．具体的には，射影測定の結果が i のとき，i 番めの量子ビットに σ_z を作用する（$i = 0$ のときは何もしない）．

この手順により，符号ベクトルと環境とのエンタングルメントは最終的にほどけ，また振幅 a_0, a_1 は変化しないことに注意せよ．

7.4.5 量子ハミング限界

次に，より一般的な量子ビット－環境のエンタングルメント

$$ |0\rangle|E\rangle \longrightarrow |0\rangle|E_{00}\rangle + |1\rangle|E_{01}\rangle \qquad |1\rangle|E\rangle \longrightarrow |0\rangle|E_{10}\rangle + |1\rangle|E_{11}\rangle \tag{7.51} $$

を訂正可能な符号について考える．量子ビットが重ね合わせ状態のとき，

$$ \begin{aligned} (a_0|0\rangle + a_1|1\rangle)\,|E\rangle \longrightarrow\; & (a_0|0\rangle + a_1|1\rangle)\,|E_0\rangle + \sigma_x\,(a_0|0\rangle + a_1|1\rangle)\,|E_x\rangle \\ & + \sigma_z\,(a_0|0\rangle + a_1|1\rangle)\,|E_z\rangle + \sigma_y\,(a_0|0\rangle + a_1|1\rangle)\,|E_y\rangle \\ =\; & (a_0|0\rangle + a_1|1\rangle)\,|E_0\rangle + (a_0|1\rangle + a_1|0\rangle)\,|E_x\rangle \\ & + (a_0|0\rangle - a_1|1\rangle)\,|E_z\rangle + (a_0|1\rangle - a_1|0\rangle)\,|E_y\rangle \end{aligned} \tag{7.52} $$

と書ける．ここで，σ_x はビット反転に対応するエラー演算子，σ_z は位相反転に対応するエラー演算子，$\sigma_y = -i\sigma_z\sigma_x$ は両方のエラーに対する演算子である．式 (7.52) を見てわかるように，一般の量子ビット－環境の相互作用は，量子ビットに単位行列およびパウリ演算子 $\sigma_x, \sigma_y, \sigma_z$ を作用した状態の重ね合わせとして表現される．つまり，量子ビットの状態は，エラーが生じていない状態と 3 種類のエラーが生じた状態の重ね合わせに時間発展する．

さて，非縮退符号に対する量子ハミング限界を求める [355]（一般の量子符号に対しては，より緩い条件が成立する [323]）．2^q 個の符号ベクトルから構成される符号が，η 個までのエラーを訂正可能であるとする．このとき，符号ベクトル $|\mathbf{w}\rangle$ と $|\mathbf{W}\rangle$ に η 個までのエラー演算子を作用したすべての状態は，互いに直交しなければならない．環境との相互作用により，各符号ベクトルは

$$\begin{aligned}|\mathbf{w}\rangle|E\rangle \longrightarrow |\mathbf{w}\rangle|E_0\rangle &+ \sum_{i,k_i}|\mathbf{w}_i^{k_i}\rangle|E_i^{k_i}\rangle \\ &+ \sum_{ij,k_ik_j}|\mathbf{w}_{ij}^{k_ik_j}\rangle|E_{ij}^{k_ik_j}\rangle + \sum_{ijl,k_ik_jk_l}|\mathbf{w}_{ijl}^{k_ik_jk_l}\rangle|E_{ijl}^{k_ik_jk_l}\rangle + \cdots \qquad (7.53)\end{aligned}$$

のように時間発展する．ここで $i, j, \cdots$ は符号ベクトル中の量子ビットの位置を表す．また $k_i, k_j, \cdots = x, y, z$ は対応する量子ビットに生じたエラーを表す．もし符号が η 個までのエラーを訂正可能であったとする．そのとき，2^q 個の符号ベクトルに η 個までのエラーが生じた状態は，すべて互いに直交している必要がある．そのため直交状態の数は，n 量子ビットのヒルベルト空間の次元より小さくなくてはいけない．したがって

$$2^q\sum_{i=0}^{\eta}3^i\begin{pmatrix}n\\i\end{pmatrix} \leq 2^n \longrightarrow 2^{n-q} \geq \sum_{i=0}^{\eta}3^i\begin{pmatrix}n\\i\end{pmatrix} \qquad (7.54)$$

が得られる．この量子ハミング限界は，η 個までのエラーを訂正可能な量子符号の検査ビット数 $n-q$ に対する下限を与える．式 (7.54) 中の因子 3^i は，量子系の場合 3 種類の独立なエラー $(\sigma_x, \sigma_y, \sigma_z)$ が各量子ビットに発生することに起因する．一方，古典系の場合はビット反転エラー (σ_x) しか生じない．

7.4.6　7 量子ビット符号

次に，任意の 1 量子ビットエラーを訂正可能な量子符号について説明する．量子ハミング限界からわかるように，最適な符号として 5 量子ビット符号 [323,356] が存在する[6]．しかし教育的理由により，Steane によって提案された 7 量子ビット符号 [357,358] について説明する．

---

[6]訳注：量子ハミング限界 (7.54) に，訂正したいエラーの数 $\eta = 1$ と情報ビット数 $q = 1$ を代入すると，$2(1 + 3n) \leq 2^n$ が得られる．この不等式を満足する最小の n は 5 である．

まずはじめに，以下のパリティ検査行列

$$\mathbf{M} = \begin{pmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{pmatrix} \tag{7.55}$$

について考える．行列 $\mathbf{M}$ のすべての列は異なっている．したがって，もし単一のビット反転エラーしか生じないのであれば，シンドローム測定によってどこの量子ビットにエラーが生じたかがわかる．符号ベクトルを構築するために，パリティ検査方程式 $\mathbf{Mu} = 0$ を満足する古典系列 $\mathbf{u}$ を利用する．この古典系列を基にして，7 量子ビットの状態 $|\mathbf{u}\rangle$ を作る．符号ベクトル $|\mathbf{w}_0\rangle(|\mathbf{w}_1\rangle$ は，$|\mathbf{u}\rangle$ の中で 1 の数が偶数個（奇数個）の状態を重ね合わせた状態として定義される．

$$|\mathbf{w}_0\rangle = \sum_{even} |\mathbf{u}\rangle_e \qquad\qquad |\mathbf{w}_1\rangle = \sum_{odd} |\mathbf{u}\rangle_o \tag{7.56}$$

なお，この符号ベクトルはエンタングル状態である．

次に，シンドローム測定について説明する．シンドローム測定を行うために，3 個の補助量子ビット（アンシラ）を追加する．各ビットはそれぞれ行列 $\mathbf{M}$ の行に対応する（図 7.5）．行列要素が $\mathbf{M}_{i,j} = 1$ のとき，CNOT ゲートを導入する．そのとき，i 番めの補助量子ビットを標的ビットに，符号ベクトルの j 番めの量子ビットを制御ビットにする．

符号ベクトルおよび補助ビットの初期状態をそれぞれ $|\mathbf{v}\rangle$ および $|0\rangle$ とする．このとき，補助ビットの最終状態は，シンドロームの値に対応する状態 $|\mathbf{s}\rangle = |\mathbf{Mv}\rangle$ となる．

$$|\mathbf{v}\rangle \otimes |0\rangle_{anc} \longrightarrow |\mathbf{v}\rangle \otimes |\mathbf{Mv}\rangle_{anc} \tag{7.57}$$

1 量子ビットのビット反転エラーしか生じないと仮定する．補助ビットを観測することにより，符号ベクトルは正しい状態か 1 量子ビットが反転した状態かのどちらかに射影される．さらに，補助ビットの値からエラーが生じた量子ビットの位置がわかる．このエラーは，演算子 σ_x を作用することによって訂正できる．

上で紹介した方法は，位相反転エラーの訂正にも拡張できる．その際，基底 $|0\rangle, |1\rangle$ における位相反転は，それをアダマール変換した基底 $|\bar{0}\rangle, |\bar{1}\rangle$ におい

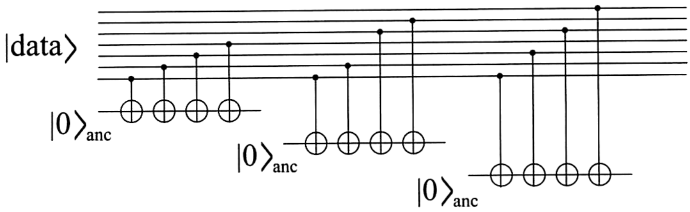


図 **7.5**　7 量子ビット符号におけるビット反転シンドロームの測定

てはビット反転になることに注意する[7]．したがって，回転した基底でビット反転を訂正すればよい．もしビットごとにアダマール変換 H を作用すれば，各量子ビットは

$$|0\rangle \longrightarrow |\tilde{0}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \longrightarrow |\tilde{1}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{7.58}$$

と変換され，符号ベクトルは

$$|\mathbf{w}_0\rangle \longrightarrow |\tilde{\mathbf{w}}_0\rangle \equiv \frac{1}{\sqrt{2}}(|\mathbf{w}_0\rangle + |\mathbf{w}_1\rangle), \quad |\mathbf{W}_1\rangle \longrightarrow |\tilde{\mathbf{w}}_1\rangle \equiv \frac{1}{\sqrt{2}}(|\mathbf{w}_0\rangle - |\mathbf{w}_1\rangle) \tag{7.59}$$

となる．ここで $|\tilde{\mathbf{w}}_0\rangle$ と $|\tilde{\mathbf{w}}_1\rangle$ はパリティ検査方程式を満足することに注意せよ．したがって，位相エラーを訂正する方法は以下のようになる（図 7.6）．符号ベクトルの各ビットごとにアダマール変換 H を作用する．そして，変換した基底でビット反転エラーを訂正する．最後に，もとの基底 $|0\rangle, |1\rangle$ に戻すためにアダマール変換 H を作用する．このようにして位相エラーは訂正される．したがって，7 量子ビット符号を用いることによって，1 量子ビットの任意のエラー（位相エラー，ビットエラー，位相およびビットエラー）を訂正することができる．

7.4.7　フォールトトレラント量子計算

いままで，計算中にエラーは生じないと仮定してきた．しかし，実際はゲート演算中にもエラーは生じる．さらに，符号化，復号化，エラー訂正も一種のゲート演算である．そのため，不完全な量子回路を用いて信頼できる計算を行う方法について考える必要がある．そこで，この節ではフォールトトレ

---

[7] 訳注：$H\sigma_z H = \sigma_x$（H はアダマール変換）より，$H\sigma_z|0\rangle = H\sigma_z HH|0\rangle = \sigma_x|\tilde{0}\rangle$．

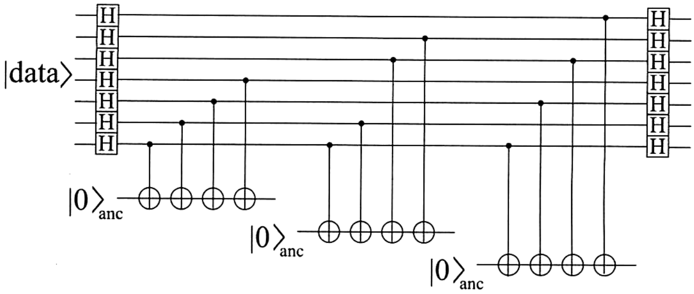


図 **7.6**　7 量子ビット符号における位相反転シンドロームの測定

ラント量子計算 [359] の基本概念について説明する．不完全ゲート演算によってエラーが他のビットに伝染することを見るために，補助ビットを用いたシンドローム測定について考える．補助量子ビットは，いくつかの CNOT ゲートの標的ビットである（図 7.5）．量子 CNOT ゲートにおいては，標的ビットに作用する位相エラーは，制御ビットに影響を与える．そのため，補助量子ビットにおける位相エラーは，1 個以上のデータ量子ビットに伝染する．しかし，前節で紹介した量子エラー訂正符号は，1 個のエラーしか訂正できないことに注意せよ．したがって，補助ビットが二つのデータ量子ビットを汚染してしまうと，エラーを訂正できない．

エラー伝染を抑える一つの方法は，各データ量子ビットの標的ビットとして，それぞれ別々の補助ビットを用いることである．このときシンドロームビットは，補助ビットの一括測定の結果から推定する．しかし，そのような測定はエラー情報のみを与え，データ量子ビットに関する情報を与えないことを確かめる必要がある．その解答は Shor によって与えられた．Shor の方法においては，補助ビットは 1 の数が偶数個の状態の重ね合わせとして用意される．

$$|Shor\rangle = \sum_{even} |\mathbf{x}\rangle \tag{7.60}$$

たとえば 7 量子ビット符号の場合，補助量子ビットの初期状態は

$$\begin{aligned}|Shor\rangle = \frac{1}{\sqrt{8}}(&|0000\rangle + |0011\rangle + |0101\rangle + |1001\rangle + |0110\rangle + |1010\rangle \\ &+ |1100\rangle + |1111\rangle)\end{aligned} \tag{7.61}$$

である．

各補助ビットは，異なるデータ量子ビットの標的ビットである（図 7.7）．補助ビットのパリティを測定することにより，シンドロームビットの値が得られる．この方法により，補助ビット測定はエラーに関する情報のみしか与えないことが保証される．さらに補助ビットのエラーは，データ量子ビットに広がらないことも保証される．

しかしながら，われわれの目的は情報の保存だけでなく，そのデータに対して計算を行うことである．もっとも簡単な方法は，データを復号してから計算を行い，また符号化するというものである．しかし，復号してから符号化するまでの間，データはエラーに対して無防備である．したがって，量子ビットを保護するために，符号ベクトルに対して直接計算を行う必要がある．さらに，エラーの伝染を避けるために，この計算をフォールトトレラントに行わなければばならない．符号ベクトルに対するゲート演算を 1 量子ビットごとの演算として再構成できるときは，これらの要請は自動的に達成される．式 (7.59) ですでに見たように，アダマール変換に対してはこのような構成は可能である．さらに，符号ベクトルに対する CNOT ゲートも各量子ビット毎の CNOT ゲートとして構築できる．これら二つのゲートだけでは，万能量子論理ゲート集合は構成できない．しかし，フォールトトレラントなトフォリゲートを用いることにより，万能ゲート集合が実現できる．

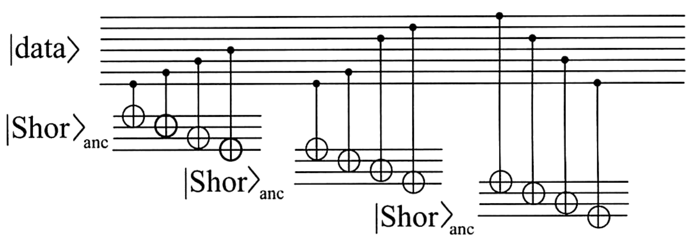


図 7.7　7 量子ビット符号におけるフォールトトレラントなシンドローム測定

7.5　量子エラー訂正とフォールトトレラント量子計算の一般論

(*A. Steane*)

前節において，量子エラー訂正 (QEC) の基礎といくつかの例について紹介

した．ここでは，より一般的な理論について簡単に紹介する．

QEC は三つの主要な概念に基づいている．それは，ノイズのデジタル化，エラー演算子とシンドロームの操作，量子エラー訂正符号 (QECC) の構築である．QEC がどの程度成功するかはノイズの物理的性質に依存する．この点については 7.5.4 項で説明する．

7.5.1 ノイズのデジタル化

「ノイズのデジタル化」とは，量子ビット系と（環境のような）他の系との**任意の**相互作用が式 (7.52) の一般形

$$|\phi\rangle|\psi\rangle_e \to \sum_i (E_i|\phi\rangle)\,|\psi_i\rangle_e \tag{7.62}$$

によって表現できるということを意味する．ここで,「エラー演算子」E_i は量子ビットに作用するパウリ演算子のテンソル積である．また $|\phi\rangle$ は量子ビットの初期状態である．$|\psi_i\rangle_e$ は環境の状態であり，必ずしも直交し規格化されているとは限らない．したがって，ノイズとデコヒーレンスまたはそれらの両方を，量子ビットに作用するパウリ演算子 σ_x, σ_y, σ_z を用いて表現する．以下，これらの演算子を $X \equiv \sigma_x, Z \equiv \sigma_x, Y \equiv -i\sigma_y = XZ$ と表す．

n 量子ビットに作用するパウリ行列のテンソル積を表現するために，表記法 $X_u Z_v$ を導入する．ここで，u と v は n ビットの 2 元ベクトルである．u と v の中で成分が 1 のビットは，テンソル積の中で演算子 X と Z が現れている位置を表す．たとえば

$$X \otimes I \otimes Z \otimes Y \otimes X \equiv X_{10011} Z_{00110} \tag{7.63}$$

である．

エラー訂正とは，状態 $E_i|\phi\rangle$ を $|\phi\rangle$ に戻す操作のことである．X エラーの訂正により，$X_u Z_v|\phi\rangle$ は $Z_u|\phi\rangle$ へ変化し，Z エラーの訂正により $X_u Z_v|\phi\rangle$ は $X_u|\phi\rangle$ へ変化する．これらを組み合わせれば，**最も一般的な**ノイズ (7.62) を訂正することができる．つまり，X および Z エラーだけを訂正すればよいのである．

7.5.2 エラー演算子，安定化部分群，シンドローム抽出

この節では，Gottesman[360] および Calderbak ら [361,362] によって提唱された方法を用いて，エラー演算子およびシンドロームの数学について説明す

る．この方法は，Steane[357,358] および Calderbank と Shor[363,364] によって発見された方法を基礎としている．

単位行列と三つのパウリ演算子から構成される集合 $\{I, X, Y, Z\}$ について考える．パウリ演算子を 2 乗すると単位行列 I になる ($X^2 = Y^2 = Z^2 = I$)．またパウリ演算子の固有値は ± 1 である．集合内の任意の二つの要素は，可換（たとえば，$XI = IX$）であるか反可換（たとえば，$XZ = -ZX$）であるかのどちらかである．パウリ演算子のテンソル積（エラー演算子）も 2 乗すると I になり，またそれらは互いに可換か反可換のどちらかである．

n 量子ビットの場合，エラー演算子の**長さ** (length) は n となる．また，エラー演算子の**重み** (weight) は，単位行列 I 以外の項の数である．たとえば，$X_{10011}Z_{00110}$ の長さは 5 であり，重みは 4 である．

$\mathcal{H} = \{M\}$ を可換なエラー演算子の集合とする．この集合内の演算子はすべて可換なので，同時固有状態をもつ．また，$\mathcal{C} = \{|u\rangle\}$ を，固有値 +1 の同時固有状態の正規直交集合とする．

$$M|u\rangle = |u\rangle \qquad {}^{\forall}|u\rangle \in \mathcal{C}, {}^{\forall}M \in \mathcal{H} \tag{7.64}$$

集合 $\mathcal{C}$ は量子エラー訂正符号であり，$\mathcal{H}$ はその**安定化部分群** (stabilizar) である．正規直交状態 $|u\rangle$ は**符号ベクトル** (code vector) あるいは**量子符号語** (quantum codeword) と呼ばれる．以下，$\mathcal{H}$ が群を構成している場合についてのみ考察する．群 $\mathcal{H}$ は $n-k$ 個の線形独立な生成元によって生成され，元の数は 2^{n-k} である．この場合 $\mathcal{C}$ の元の数は 2^k である．そのため，$\mathcal{C}$ の元は全系の 2^n 次元ヒルベルト空間内の 2^k 次元部分空間を張る．したがって，$\mathcal{C}$ を用いて k 量子ビットの状態を n 量子ビットの状態に符号化することができる．この部分空間内の一般の状態は，**符号化状態** (encoded state) あるいは**論理的状態** (logical state) と呼ばれ，符号ベクトルの重ね合わせ状態

$$|\phi\rangle_L = \sum_{|u\rangle \in \mathcal{C}} a_u |u\rangle \tag{7.65}$$

として表現できる．

当然ながら，ある与えられた QECC を用いて，考えうるエラーすべてを訂正することはできない．それぞれの符号は，**訂正可能なエラー** (correctable error) と呼ばれる特定のエラー集合 $\mathcal{S} = \{E\}$ しか訂正できない．そのため，

考えている物理系で生じうるエラーが訂正可能な集合 $\mathcal{S}$ に含まれるように符号を構成する必要がある．この重要なテーマについては，次項で説明する．本項においては，まず最初に訂正可能なエラーと安定化部分群との関係について示す．そして，エラー訂正は実際にどのようにして行われるかについて見てみる．

安定化部分群中のエラー演算子は，すべて訂正可能である（$^\forall E \in \mathcal{H}$ に対して $E \in \mathcal{S}$）．なぜならば，これらの演算子を一般的な論理的状態 (7.65) に作用しても，状態は変化しないからである[8]．もし，考えている系のノイズがこれらの演算子のみから構成されるのであれば，QECC はノイズの影響を受けない部分空間になる．このような部分空間は，デコヒーレンスフリー部分空間 (decoherence free subspace) と呼ばれる．

一方，符号化状態を変化させるエラーの集合も存在する．にもかかわらず，これらのエラーはエラーシンドロームを抽出し，その結果に応じて系にユニタリ変換を作用することによって訂正可能である．以下，訂正可能なエラー集合 $\mathcal{S} = \{E_i\}$ においては，すべての演算子の積 E_1E_2 が，$\mathcal{H}$ に含まれるか $\mathcal{H}$ の元と反可換であるかのどちらかであることを示す．これを見るために，まずはじめに後者の場合

$$\text{ある } M \in \mathcal{H} \text{ に対して} \quad E_1E_2M = -ME_1E_2 \tag{7.66}$$

について考える．このような結合エラー演算子 E_1E_2 は**検出可能** (detectable) であるという．これは，

$$\begin{aligned} &\{ME_1 = -E_1M, ME_2 = E_2M\} \quad \text{か} \\ &\{ME_1 = E_1M, ME_2 = -E_2M\} \quad \text{のどちらか} \end{aligned} \tag{7.67}$$

の場合にのみ生じる．シンドロームを抽出するために，安定化部分群中のすべてのオブザーバブルを測定する．これを行うためには，$\mathcal{H}$ 中の $n-k$ 個の線形独立な M（$\mathcal{H}$ の生成元）を測定するだけで十分である．符号化部分空間内の状態は，すでにこれらの演算子すべての固有状態である．したがって，これらの状態は測定によって影響を受けない．一方エラーが生じた状態は，測定により各 M の固有値 ±1 の固有状態に射影される．これら $n-k$ 個の固有

[8]訳注：$^\forall E \in \mathcal{H}$ に対して $E|\phi\rangle_L = \sum_{|u\rangle \in C} a_u E|u\rangle = \sum_{|u\rangle \in C} a_u|u\rangle = |\phi\rangle_L$.

値列がシンドロームである．式 (7.67) により，E_1 と E_2 のシンドロームは異なることが保証される．したがって，E_1 と E_2 は互いに区別可能である．エラーが生じた状態 $E|\phi\rangle_L$ のオブザーバブル M を測定することを考える．式 (7.67) より $E = E_1$ と $E = E_2$ の場合とで，異なる固有値が得られる．したがって，エラーをシンドローム（固有値）から推定することができる．そして，（エラー演算子は 2 乗すると単位行列になるので）推定されたエラーを系に再び作用することによってエラー訂正が行われる．

次に，一般的な符号化状態に対するエラー訂正過程について見てみる．ノイズが生じた状態は

$$\sum_i \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e \tag{7.68}$$

である．シンドローム抽出は，最も単純には以下のようにして行われる．まず，$n-k$ 量子ビットのアンシラ a を系に追加する．そして，CNOT ゲートとアダマールゲートから構成される回路によって固有値をアンシラに保存する．厳密な量子ネットワークは，アンシラに保存されているパリティ検査情報について考察することにより構成できる（たとえば図 7.5）．あるいは，以下に示す標準的な固有値測定方法によっても構成できる．演算子 M の固有値 $\lambda = \pm 1$ を抽出するためには，まずアンシラを状態 $\left(|0\rangle + |1\rangle\right)/\sqrt{2}$ に用意する．次に，アンシラを制御ビット，系を標的ビットとして制御 M ゲートを作用する．最後にアンシラにアダマールゲートを作用すると，アンシラの最終状態は $\left[(1+\lambda)|0\rangle + (1-\lambda)|1\rangle\right]/2$ となる[9]．このプロセスを $n-k$ 個の演算子 $M(\in \mathcal{H})$ に対して実行することにより，状態は

$$|0\rangle_a \sum_i \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e \rightarrow \sum_i |s_i\rangle_a \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e \tag{7.69}$$

と変化し，系と環境がアンシラとエンタングルする．s_i は $(n-k)$ ビットの 2 元系列である．もし，E_i のシンドロームが i ごとにすべて異なっていれば，s_i はすべて異なっている．アンシラの射影測定によって，式 (7.69) は和の中のどれか一つの状態 $|s_i\rangle_a \left(E_i|\phi\rangle_L\right)|\psi_i\rangle_e$ にランダムに変化する．そして，測定結果として s_i が得られる．このシンドロームをもつ E_i は一つしかない．し

[9] 訳注：固有値 λ が $1(-1)$ の場合，アンシラの状態は $|0\rangle(|1\rangle)$ となる．したがって，アンシラを基底 $\{|0\rangle, |1\rangle\}$ で測定することにより固有値がわかる．

たがってエラー演算子 E_i を推定でき，E_i を系に作用することによりエラーを訂正できる！

この注目すべき過程は以下のようにして理解することができる．まず，射影測定によってエラー集合の中から一つのエラーが「選ばれる」．そして，測定結果からどのエラーが生じたかわかるので，その「選ばれた」離散的エラーを反転する．別の言い方をすれば，エラー訂正は（環境とのエンタングルメントを含む）ノイズを系からアンシラに効果的に移す（制御ビットがアンシラで標的ビットが系の制御ゲートから構成される）ユニタリ発展によって達成される．

次に，(7.66) の直前で述べたもう一つのエラーの可能性について議論する．すなわち

$$E_1 E_2 \in \mathcal{H} \tag{7.70}$$

について考える．この場合，E_1 と E_2 のシンドロームは等しいので，シンドロームの抽出によって，これらのエラーを区別することはできない．しかし，これは問題とはならない！　このシンドロームが得られた場合，単に演算子 E_1 を作用すればよい．もし生じたエラーが E_1 であれば，明らかに問題はない．一方，E_2 が生じていた場合，最終状態は $E_1 E_2|\phi\rangle_L$ となりエラーのない状態となる！[10]　古典符号理論においては，これに類似する状況はない．このような量子符号は，**縮退** (degenerate) 符号と呼ばれ，量子ハミング限界 (7.54) によって制限されない．

安定化部分群による議論は，状態よりもむしろ演算子に注目しているので非常に有用である．にもかかわらず，量子符号語は非常に興味深い状態である．なぜならば，多くの対称性および興味深い形のエンタングルメントをもつからである．量子符号語がエラー集合 $\mathcal{S}$ を訂正可能であるための必要十分条件は，すべての $E_1, E_2 \in \mathcal{S}$ および $|u\rangle, |v\rangle \in \mathcal{C}$，$|u\rangle \neq |v\rangle$ に対して

$$\langle u|E_1 E_2|v\rangle = 0 \tag{7.71}$$

$$\langle u|E_1 E_2|u\rangle = \langle v|E_1 E_2|v\rangle \tag{7.72}$$

で与えられる [323,365]．$E_1 E_2$ が安定化部分群の元と常に反可換であるとき，$\langle u|E_1 E_2|u\rangle = \langle u|E_1 E_2 M|u\rangle = -\langle u|M E_1 E_2|u\rangle = -\langle u|E_1 E_2|u\rangle$ となる．した

[10] 訳注：$E_1 E_2 \in \mathcal{H}$ より $E_1 E_2|\phi\rangle_L = |\phi\rangle_L$．

がって，$\langle u|E_1E_2|u\rangle = 0$ が得られる．これは非縮退符号である．つまり，すべての符号ベクトルおよびそれにエラーが生じた状態は互いに直交し，符号は量子ハミング限界を満足する．

7.5.3　符号の構築

符号の構築はそれ自身，緻密で興味深い研究分野である．そこで，本項において符号の構築法について簡単に紹介する．

まずはじめに，安定化部分群の元はすべて互いに可換であることを思い出そう．一方，$X_uZ_v = (-1)^{u\cdot v}Z_vX_u$ を簡単に示すことができる．ここで，$u\cdot v$ は 2 元のパリティ検査演算，つまり GF(2) 上の 2 元ベクトルの内積である[11]．この式から，$M = X_uZ_v$ と $M' = X_{u'}Z_{v'}$ が可換であるための必要十分条件は

$$u \cdot v' + v \cdot u' = 0 \tag{7.73}$$

であることがわかる．安定化部分群は，$n-k$ 個の線形独立なエラー演算子によって完全に記述できる．これらの演算子を，二つの $(n-k)\times n$ 2 元行列 H_x, H_z を用いて表すと便利である[12]．したがって，安定化部分群 $\mathcal{H}$ は，$(n-k)\times 2n$ 2 元行列

$$H = (H_x|H_z) \tag{7.74}$$

によって一意に表すことができる．また，すべての演算子が可換（すなわち $\mathcal{H}$ がアーベル群）であるという条件は

$$H_xH_z^T + H_zH_x^T = 0 \tag{7.75}$$

と表現できる．ここで，^{T} は行列の転置である．

行列 H は，古典エラー訂正符号のパリティ検査行列に類似している．生成行列の類似物は，

$$H_xG_z^T + H_zG_x^T = 0 \tag{7.76}$$

を満足する行列 $G = (G_x|G_z)$ である．別の言い方をすれば，H と G は，式 (7.73) で定義される内積に関して双対な関係にある．G の行の数は $n+k$ であり，G から直接 H を得ることができる．

[11]訳注：GF(2) とは，元の数（位数）が 2 のガロア体（有限体）のこと．
[12]訳注：行列 $H_x(H_z)$ の i 行めは，i 番めのエラー演算子の $u(v)$ である．

式 (7.75) および式 (7.76) より，G は H に含まれることがわかる．そこで $\mathcal{G}$ を，G により生成されるエラー演算子の集合とする．このとき，$\mathcal{G}$ もまた $\mathcal{H}$ に含まれる．

定義 (7.76) により，$\mathcal{G}$ のすべての元は $\mathcal{H}$ のすべての元と可換である．また，$\mathcal{H}$ のすべての元と可換な演算子はこれ以外に存在しない．したがって，$\mathcal{G}$ に含まれないすべてのエラー演算子は，少なくとも $\mathcal{H}$ の一つの元と反可換である．これにより以下の強力な結果が得られる．もし，(単位行列以外の) $\mathcal{G}$ のすべての元の重みが少なくとも d であるとすると，重みが d 以下の（単位行列以外の）すべてのエラー演算子は $\mathcal{H}$ のある元と反可換である．したがって，これらのエラー演算子は検出可能である．そのため，そのような符号は重みが $d/2$ 以下のすべてのエラー演算子を訂正可能である．

もし，重み d 以下の $\mathcal{G}$ の元だけが，$\mathcal{H}$ の元であった場合はどうなるのであろうか．このときも性質 (7.70) から，符号は重み $d/2$ 以下のすべてのエラー演算子を訂正可能であることがわかる（縮退符号）．重み d は，符号の最小距離 (minimum distance) と呼ばれる．

したがって符号構築の問題は，式 (7.75) を満足する行列 H と式 (7.76) によって定義される双対行列 G を見つけるという問題に帰着される．よく知られた古典エラー訂正符号を用いてそのような符号を構築することができる．

$$H = \left(\begin{array}{c|c} H_2 & 0 \\ 0 & H_1 \end{array}\right), \qquad G = \left(\begin{array}{c|c} G_1 & 0 \\ 0 & G_2 \end{array}\right) \tag{7.77}$$

ここで，$H_i (i = 1, 2)$ は G_i によって生成される古典符号 C_i の検査行列である．したがって $H_i G_i^T = 0$ と式 (7.76) を満足する．可換条件 (7.75) を満足するためには $H_1 H_2^T = 0$ でなければいけない．つまり $C_2^\perp \subset C_1$ でなければいけない．もし古典符号のビット数が k_1, k_2 であれば，量子符号のビット数は $k = k_1 + k_2 - n$ となる．このとき，量子符号は

$$|u\rangle_L = \sum_{x \in C_2^\perp} |x + u \cdot D\rangle \tag{7.78}$$

で与えられる．ここで u は k ビットの符号語，x は n ビットの符号語である．また D は剰余類代表元 (coset leader) の $(k \times n)$ 行列である．この符号は CSS(Calderbank-Shor-Steane) 符号と呼ばれる．この符号は効率的であり，

フォールトトレラント量子計算において役に立つので重要である（以下を見よ）.

符号が「効率的」であるとは，ある d/n に対して $k, n, d \to \infty$ とするとき，符号化率 k/n がある下限よりも上に漸近するような符号が存在するということである．CSS 符号の最小距離は $d = \min(d_1, d_2)$ となる．もし $C_1 = C_2 = C$ であれば $C^\perp \subset C$ となる．そのような符号は自己双対符号 (self-dual code) と呼ばれる．自己双対符号の符号化率に対しては，ある有限の下限が存在することが知られている [364]．これはとても重要なことであり，QEC はノイズを抑制するための大変強力な方法であると言える（次節を見よ）.

CSS 符号よりもさらに効率的な QECC も存在する．その符号は，CSS 符号の拡張あるいは別の方法により得られる．この節の最後に，例として $[[n, k, d]] = [[5, 1, 3]]$ 最適符号の安定化部分群と生成行列を示す．この符号は，1 量子ビット $(k = 1)$ を 5 量子ビット $(n = 5)$ に符号化する．そして，この符号により，($d/2 = 1.5$ なので）重み 1 以下のすべてのエラーを訂正することができる.

$$H = \begin{pmatrix} 11000 & 00101 \\ 01100 & 10010 \\ 00110 & 01001 \\ 00011 & 10100 \end{pmatrix}, \qquad G = \begin{pmatrix} H_x & H_z \\ 11111 & 00000 \\ 00000 & 11111 \end{pmatrix} \tag{7.79}$$

7.5.4　ノイズの物理

ノイズとデコヒーレンスは，それ自身広大な研究テーマである．この項においては，いくつかの基本概念について簡単に説明する．そして，QEC ができることとできないことを明らかにする.「ノイズ」とは，系の密度行列に対する未知の望ましくない変化のことを意味する.

ノイズがデジタル化できること（式 (7.62)）は，任意の量子ビット－環境の相互作用が

$$H_I = \sum_i E_i \otimes H_i^e \tag{7.80}$$

の形に書けることと等価である．ここで，H_i^e は環境に作用する演算子である．この相互作用の下で,（環境をトレースアウトした）系の密度行列は ρ_0 から $\sum_i a_i E_i \rho_0 E_i$ へ時間発展する．QEC を用いることにより，この和の中で訂

正可能な E_i の項すべてが ρ_0 に戻る．したがって，(ノイズのない状態 ρ_0 と比較した）訂正後の状態の忠実度は，訂正不可能なエラーに対応する係数 a_i の和によって決定される．

この問題に対する数学的に詳細な解析については，文献 [365,366] を見よ．重要なアイデアは以下のとおりである．ノイズは，全量子ビットに常に作用する一つの連続プロセスである．しかし QEC について議論するとき，シンドロームは射影測定によって得ることができるとしてよい．したがって，たとえば「エラー E_i が発生する確率」とは,「シンドローム抽出によって，エラー E_i が作用した状態に射影される確率」を短く表現したものである．そこで以下，その確率を計算する．

そのためには，式 (7.80) を重みが等しいエラー演算子の項ごとに分けると便利である．

$$H_I = \sum_{\mathrm{wt}(E)=1} E \otimes H_e^E + \sum_{\mathrm{wt}(E)=2} E \otimes H_e^E + \sum_{\mathrm{wt}(E)=3} E \otimes H_e^E + \cdots \quad (7.81)$$

第 1 項の和の項数は $3n$，第 2 項の項数は $3^2 n!/(2!(n-2)!)$ である．量子系－環境の結合の強さは，演算子 H_E^e の中に現れる結合定数によって表される．重み 1 の項しか存在しないとき，環境は各量子ビットに対して独立に作用するとしてよい．つまり，環境は 2 量子ビット以上にわたって相関したエラー (correlated error) を直接発生しない．無相関エラーが生じる場合でも，すべての重みのエラーが密度行列の中に現れるであろう．しかし，重みが w である項の大きさは $O(\epsilon^{2w})$ となる．ここで ϵ は結合強度に関係するパラメータである．

QEC を用いることにより，密度行列の中で重み $t = d/2$ 以下の項すべてが元に戻る．無相関ノイズモデルにおいては，訂正後の状態の忠実度は，$1-P(t+1)$ で与えられる（$P(t+1)$ は重み $t+1$ のエラー発生確率）．すべての 1 量子ビットエラーの寄与をコヒーレントに足し上げられるとき（つまり，すべての量子ビットが同じ環境と相互作用するとき），この確率は近似的に

$$P(t+1) \simeq \left(3^{t+1} \begin{pmatrix} n \\ t+1 \end{pmatrix} \epsilon^{t+1}\right)^2 \quad (7.82)$$

と書ける．一方，エラーをインコヒーレントに足し上げるとき（すなわち，各量子ビットがそれぞれ独立な環境と相互作用する，あるいは同じ環境と相互

作用するが結合の位相がランダムなとき）

$$P(t+1) \simeq 3^{t+1} \binom{n}{t+1} \epsilon^{2(t+1)} \tag{7.83}$$

と書ける．式 (7.82) と (7.83) により，t が大きく $\epsilon^2 < t/3n$ の場合，QEC は非常によく機能することがわかる．よい符号が存在するので，t/n と k/n を一定にしたままで，t を実際無限大にすることができる．したがって，1 量子ビットあたりのノイズが閾値（約 $t/3n$）以下であれば，ほぼ完全に状態を回復することができる．ただし，t/n は，量子ハミング限界によって符号化率 k/n を制限する．

上で述べた無相関ノイズモデルは，多くの物理的状況において妥当な近似である．しかし，ϵ^d のオーダの大変小さな項について考えているので，近似の程度について注意する必要がある．完全無相関ノイズの近似を緩めるとする．重み t のエラーに対する式 (7.81) の結合定数が $\epsilon^t/t!$ のオーダのときだけ，式 (7.82) と (7.83) はほとんど変化しない．

相関エラー（バーストエラー）が量子系－環境の結合を支配している場合でも，QEC はうまく機能する．しかし，すべての相関エラーを含む安定化部分群から構成される別の種類の QEC を見つけることができる．これは,「エラー訂正」というよりはむしろ「エラー回避 (error avoiding)」と呼ばれる．なぜならば，そのような符号はもともと環境と結合していないので，エラー訂正の必要がないからである．以上により，環境と（系と環境の）結合の構造について知れば知るほど，よりよい符号を見つけられるということがわかった．

7.5.5　フォールトトレラント量子計算

いままで議論してきた QEC の方法は，ノイズの存在する量子通信路を用いた高忠実度通信に適している．しかし，それが量子計算に適しているかどうかはまだ明らかではない．なぜならば，いままでの議論において，シンドローム抽出の量子演算中にエラーは生じないと仮定してきたからである．

実際は，基本量子演算や自由時間発展のときでもノイズが存在する．フォールトトレラント量子計算とは，そのような状況においても信頼できる量子情報処理のことである．そのための一つの方法として，QEC を繰り返し使うということがあげられる．しかし，シンドローム抽出中に生じたエラーも訂正

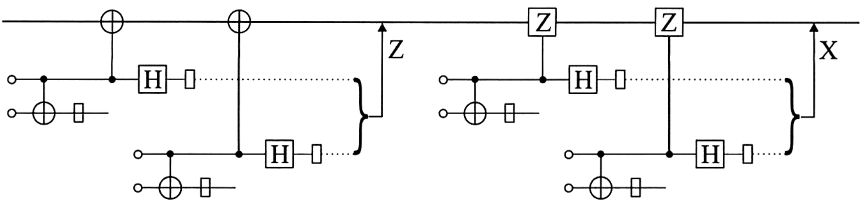


図 **7.8** フォールトトレラントシンドローム抽出ネットワーク

できるように注意深く設計する必要がある．本質的に新しい方法が Shor[367] によって提案され，Preskill[359] によって議論された（[368]-[370] も参照のこと）．その後，Steane[371,372] によって重要な改良がなされたのであるが，ここでは Shor の方法について紹介する．フォールトトレラント量子計算の分野は，QEC に比べてまだ未発達である．そのため，多くの方法がまだ詳細に調べられていない．そこで，この節においてはシンドロームを正確に抽出する一つの方法のみについて説明する．

完全なフォールトトレラントシンドローム抽出ネットワークを図 7.8 に示す．簡単のために，最も単純な単一量子エラー訂正符号の場合についてのみ考える（多数のエラーを訂正する符号への一般化も可能である）．コンピュータ内の 2 準位系のことを物理的量子ビットと呼ぶ．ネットワーク中の各直線は，1 量子ビットではなく n 量子ビットのブロックを表す．アダマールゲートあるいは CNOT ゲートのような演算は，関連するブロックあるいはブロック対に作用する n 量子ビット演算子である．

この方法は，注意深く手続きを繰り返すこと，X エラーと Z エラーの伝染の仕方は異なるという事実，CSS 符号の有用な性質に依存している．エラーは，物理的 1 あるいは 2 量子ビットに対する（状態準備と測定を含む）ゲート演算中か自由時間発展中に生じると定義する．また，ノイズは相関がなく確率的であると仮定する．そのためエラーは確率 $\sim\gamma$ で独立に生じる．図 7.8 のネットワークの目的は，計算ブロック中の 1 量子ビットエラーの訂正である．その際，ある 1 量子ビットエラーによって，計算ブロック中に重み 2 以上のエラーが生じないようにする．重要なことは，$O(\gamma)$ の確率で，訂正不可能なエラーを生じさせないということである．

そのために，まず二つのアンシラブロックを用意する．そして，それぞれを論理的ゼロ状態 $|0\rangle_L$ に準備する．この準備過程はフォールトトレラントで

はない．準備された状態は $O(\gamma)$ の確率で任意の重みのエラーを含む．そのため，この準備過程はある確率で失敗する．次に，二つのアンシラブロック間に CNOT 演算を作用する．そして，一つのブロック内の全量子ビットを計算基底で観測する．これによって，正しい状態が用意されたかどうかを確認しているのである．その際，ブロック間の物理的 CNOT は，CSS 符号に対する論理的 CNOT になっているという事実を利用する．したがって，測定結果は古典符号 $C_2^\perp$(7.78) の一つの元になっているであろう．もしそうでなければ，もう一度アンシラ対を用意し直す．そして，測定結果が $C_2^\perp$ の元になるまでこの過程を繰り返す．この段階で，測定しなかったアンシラに重み 2 以上の X エラーが生じている確率は $O(\gamma^2)$ である．なぜならば，それはエラーが少なくとも二つの位置に発生する場合に起こるからである．ただし，アンシラに任意の重みの Z エラーが生じている可能性があることに注意せよ．

次に，確認したアンシラと量子コンピュータとを，ブロックごとの物理的 CNOT によって結合する．ここでまた，この演算は符号語に対する論理的 CNOT になることを利用した．そのため，(アンシラが制御ビットなので) 何も起こらないであろう！　しかし実際は，X エラーがアンシラからコンピュータに伝染する，あるいは Z エラーがコンピュータからアンシラに伝染するといったことが生じる．これは，Z エラーのシンドロームをアンシラに集めるフォールトトレラントな方法の一つである．シンドロームの読み出しは，まず（Z エラーを X エラーに変換するために）アンシラにアダマール変換 H を施し，次にアンシラの全ビットを計算基底で観測することによって行われる．ここで，ブロックごとの物理的 H は論理的 H として機能するという（いくつかの種類の CSS 符号に対して成立する）性質を用いた．そのため，アダマール変換 H を作用しても，アンシラ状態は（X エラーに変換される Z エラーを除いて）符号化部分空間中の状態のままである．

量子コンピュータ内に重み 2 のエラーを発生できる単一エラーの位置はもうない．しかし，1 量子ビットエラーのために正しくないシンドロームが得られる危険性が残っている．もし，間違ったシンドロームに基づいて訂正を行えば，さらなるエラーが発生するであろう．したがって，いままで説明してきた全過程を繰り返し，最終的に二つのシンドロームを得る．もしその二つが一致していたとする．どちらも間違っているのは，二つの異なる位置でエラーが生じた場合のみである．しかし，それは $O(\gamma^2)$ の過程であるので，シ

ンドロームは正しいとしてよい．もしシンドロームが一致しなければ，もう一度全過程を繰り返し，3 個めのシンドロームを得る．そして，多数決によってシンドロームを決定する．

以上により，量子コンピュータ中の Z エラーの訂正が完了した．ネットワークの残り半分は同様に動作し，量子コンピュータ中の X エラーを訂正する．

上記の過程は，X エラーと Z エラーの伝染の仕方は異なるということに依存する．X エラーに対しては，フォールトトレラントにアンシラを確認できる．ところが，これにはアンシラ中に大きな重みの Z エラーが生じるという危険性が伴う．しかし，これは問題ではない．なぜならば，これらの Z エラーはもとの場所にとどまり，量子コンピュータ中に伝染しないからである．そのため，シンドロームが間違えるだけである．そこで，この間違いをもう一度シンドロームを生成することにより確認する．上記の方法はまた，(ブロックごとのゲート操作に関する）CSS 符号の性質に大きく依存していることにも注意せよ．

エラー訂正の繰り返しの各ステップにおいては，そのステップ中に生じたエラーだけでなく，それ以前のステップで生じた（訂正可能な）エラーも訂正される．一方，訂正されないエラーはそのまま残る．繰り返し回数を R とすると，エラー率は $O(R\gamma)$ から $O(R\gamma^2+\gamma)$ に抑制される．つまり，R が大きく γ が十分小さいときに役に立つ．

フォールトトレラントな計算を行うためには，望ましい量子アルゴリズムに基づいて量子状態を時間発展させなければならない．CSS 符号によって符号化された状態（論理的状態）に対する論理的アダマール変換および論理的 CNOT ゲートの実現方法についてはすでに見てきた．それぞれの物理ゲートは，1 ブロックあたり 1 個の物理的量子ビットに接続する．したがって，これらの演算はフォールトトレラントである．任意の量子論理ゲートは，基本量子ゲート集合を用いることにより近似的に表現できる．したがって，フォールトトレラントな基本量子ゲート集合を完成するためには，フォールトトレラントなトフォリゲートや制御 $\pi/2$ 回転ゲートが実現できればよい．Shor[367] は，(やや理解するのが難しい）トフォリゲートの一つのネットワークを提案した．このネットワークの構成は，量子テレポーテーションに関連している．量子テレポーテーションはフォールトトレラントな交換 (swap) 演算とみなせるので，量子コンピュータの中でフォールトトレラントに情報を転送するの

に役に立つ [372,373]．この方法やそれ以外の方法については現在活発に研究が進められている．

フォールトトレラント量子計算の実現のためには，コンピュータサイズやノイズレベルに対してかなり厳しい物理的要求がある．しかしこの文章を書いている段階では，(QEC を繰り返し用いる方法に基づく）フォールトトレラント量子計算は，大規模量子アルゴリズムを実現するための最も有望な方法と考えられる．

7.6　周波数標準

(*S.F Huelga, C. Macchiavello, M.B. Plenio, A.E. Ekert*)

この節においては，デコヒーレンスが存在するイオントラップを用いた周波数測定の精度について解析する．さまざまな測定方法だけでなく，n 個の 2 準位系のさまざまな準備方法についても考える．量子相関のない状態に対するラムゼイ分光は，最大エンタングル状態に対する最適測定と同じ精度を与えることを示す．また，対称化法を用いることによりデコヒーレンスの影響が抑制できることを示す．さらにこの方法により，初期状態準備と観測過程に関して最適化することによって得られる最適精度を超えることが可能であることを示す．

周波数標準の目的は，与えられた原子の周波数に参照発振器の周波数を安定化させることである[13]．標準的ラムゼイ干渉計を利用した原子トラップにおける光学的周波数標準の模式図を図 7.9 に示す．

まずはじめに，イオントラップ中の n 個のイオンをすべて同じ初期状態 $|0\rangle$ に用意する（$|0\rangle$ と $|1\rangle$ はそれぞれイオンの基底状態と励起状態を表す）．次に，周波数 ω のラムゼイパルスをすべてのイオンに照射する．パルス形状と幅を注意深く選ぶことにより，固有周波数 ω_0 の遷移 $|0\rangle \leftrightarrow |1\rangle$ が引き起こさ

[13] 訳注：現在の周波数標準においては，セシウム原子の基底状態の超微細構造準位が用いられる．その準位間のマイクロ波遷移周波数は 9,192,631,770Hz である．つまり，1 秒はセシウム原子のマイクロ波遷移の 9,192,631,770 周期として定義されている．このようにして定義されている 1 秒を実際に実現させる装置が周波数標準器（原子時計）である．

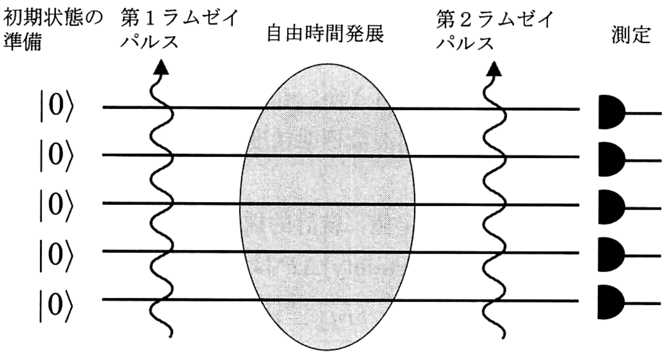


図 7.9 量子相関のない粒子を用いたラムゼイ型分光の模式図

れる．その結果，各イオンの状態は，$|0\rangle$ と $|1\rangle$ の重ね合わせ状態

$$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |1\rangle \to \frac{-|0\rangle + |1\rangle}{\sqrt{2}} \tag{7.84}$$

となる．

次に時間 t の間，系を自由に時間発展させる．発振器周波数 ω の回転座標系においては，自由時間発展はハミルトニアン

$$H = -\hbar\Delta|1\rangle\langle 1| \tag{7.85}$$

によって記述される．ここで，$\Delta = \omega - \omega_0$ は古典駆動場（参照発振器）の周波数 ω と原子遷移周波数 ω_0 との差（離調）である．このとき，基底原子状態の時間発展は

$$|0\rangle \to |0\rangle, \qquad |1\rangle \to e^{i\Delta t}|1\rangle \tag{7.86}$$

となる．したがって，周波数差 Δ によって相対位相の蓄積が生じる．次に，2 番めのラムゼイパルスを照射すると，イオンが状態 $|1\rangle$ であると観測される確率は

$$P = \frac{1 + \cos(\Delta t)}{2} \tag{7.87}$$

で与えられる．全実験時間が T となるまでこのプロセスを何度も繰り返す．そして，観測された励起状態占有率の干渉曲線から離調 Δ を推定することが

できる．この推定された Δ の値をもとにして，ω が ω_0 に等しくなるように調節する．ここで一つの疑問が生じる．原子周波数の測定において，最大どの程度の精度が達成可能なのであろうか．もっと正確に言えば，与えられた T およびイオン数 n に対して，周波数標準精度の究極限界はどうなるのであろうか．

サンプル数が有限の場合，推定値に統計的揺らぎが生じる．このとき，P の推定値に対する不確定性 (uncertainty)ΔP は

$$\Delta P = \sqrt{\frac{P(1-P)}{N}} \tag{7.88}$$

で与えられる．ここで，$N = nT/t$ は実際の実験データ数である（N は十分大きいと仮定する）．したがって，ω_0 の推定値の不確定性[14]は

$$|\delta\omega_0| = \frac{\sqrt{P(1-P)/N}}{|dP/d\omega|} = \frac{1}{\sqrt{nTt}} \tag{7.89}$$

で与えられる．これは**ショットノイズ限界** (shot noise limit)[374] と呼ばれる．この限界は技術的ノイズから生じるものではなく，量子力学固有の統計的性質から生じるものである．前者は最終的に減らすことが可能である．しかしショットノイズは，独立 n 粒子を用いた精密分光の達成可能な精度に原理的限界を与える．

最近，このショットノイズ限界を超える理論的可能性が提唱された [375,376]．基本的アイデアは，イオンの初期状態をエンタングル状態に準備するというものである．この方法の利点を見るために，2 個のイオンを最大エンタングル状態

$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{7.90}$$

に準備した場合について考えてみよう．この状態は，たとえば図 7.10 に示したネットワークの最初の部分を用いて生成することができる．つまり，第 1 イオンにラムゼイパルスを照射したあとに，CNOT ゲートを作用すればよい．時間 t の自由時間発展の後，（駆動周波数 ω の回転座標系での）相互作用表示における合成系の状態は

$$|\Psi\rangle = \frac{|00\rangle + e^{2i\Delta t}|11\rangle}{\sqrt{2}} \tag{7.91}$$

[14]訳注：周波数確度とも呼ばれる．

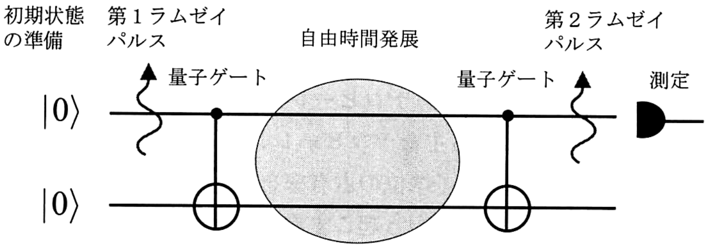


図 7.10 2量子ビットの最大エンタングル状態を用いた分光．最初の CNOT ゲートによってエンタングルメントが作り出され，2番めの CNOT ゲートによりエンタングルメントがはずされる

となる．ネットワークの最後の部分（CNOT と第2ラムゼイパルス）により，エンタングル状態が直積状態になる．第1イオンが状態 $|1\rangle$ にいる確率は，周波数 2Δ の関数として振動する．

$$P_2 = \frac{1+\cos(2\Delta t)}{2} \tag{7.92}$$

この方法は，イオン数が n 個の場合に容易に拡張できる．その際，n 個の CNOT ゲートを用いて，第1イオンと残りのイオンとをつなげればよい．このようにして，n 個のイオンの最大エンタングル状態

$$|\Psi\rangle = \frac{|00\ldots0\rangle + |11\ldots1\rangle}{\sqrt{2}} \tag{7.93}$$

が生成される．自由時間発展および CNOT ゲートの作用の後に，第1イオンを最終的に測定する．その結果，信号

$$P_n = \frac{1+\cos(n\Delta t)}{2} \tag{7.94}$$

が得られる．この方法の利点は，量子相関のないイオンを用いた場合 (7.87) に比べて，信号の振動周波数が n 倍になっていることである．そのため，周波数不確定性は

$$|\delta\omega_0| = \frac{1}{n\sqrt{Tt}} \tag{7.95}$$

となる[15]．同じイオン数 n と実験時間 T に対して，周波数不確定性がショッ

[15]訳注：ハイゼンベルグ限界と呼ばれる．

トノイズ限界 (7.89) に比べて $1/\sqrt{n}$ 倍改善されていることがわかる．またこの値は，達成可能な最大精度であることが示されている [377].

次に，現実的な実験状況，つまりデコヒーレンスが存在する場合について考える．イオントラップにおける主なデコヒーレンスは，(量子状態の相対位相をランダムに変化させるが，原子準位の占有率を変化させない）ディフェージングである．ディフェージングを引き起こす重要な原因は，衝突，迷光 (stray field)，レーザ不安定性である．デコヒーレンスが存在する場合，単一イオンの還元密度演算子 ρ の時間発展は，以下のマスター方程式 [378] によってモデル化できる．

$$\frac{d\rho}{dt} = -i\Delta\left(\rho|1\rangle\langle 1| - |1\rangle\langle 1|\rho\right) + \gamma\left(\sigma_z\rho\sigma_z - \rho\right) \tag{7.96}$$

方程式 (7.96) は，周波数 ω の回転座標系上での状態発展を記述している．$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ はパウリ演算子である．また，$\gamma = 1/\tau_{dec}$（τ_{dec} はデコヒーレンス時間）は減衰定数である．独立粒子の場合，デコヒーレンスの効果によって信号 (7.87) の広がりが生じる．

$$P = \frac{1+\cos(\Delta t)e^{-\gamma t}}{2} \tag{7.97}$$

その結果，原子周波数の不確定性は Δ に依存するようになる．

$$|\delta\omega_0| = \sqrt{\frac{1-\cos^2(\Delta t)e^{-2\gamma t}}{nTte^{-2\gamma t}\sin^2(\Delta t)}} \tag{7.98}$$

最大精度を得るために，この式を単一測定時間 t に対して最小化する必要がある．$T > \tau_{dec}/2$ と仮定すると，周波数不確定性の最小値は

$$\Delta t = \frac{k\pi}{2} \quad (k \text{ は奇数}), \qquad t = \frac{\tau_{dec}}{2} \tag{7.99}$$

の場合に達成される．したがって，周波数不確定性の最小値は

$$|\delta\omega_0|_{opt} = \sqrt{\frac{2\gamma e}{nT}} = \sqrt{\frac{2e}{n\tau_{dec}T}} \tag{7.100}$$

となる．

一方，最大エンタングル状態を準備した場合，信号 (7.94) はディフェージングの効果により以下のように変化する．

$$P_n = \frac{1+\cos(n\Delta t)e^{-n\gamma t}}{2} \tag{7.101}$$

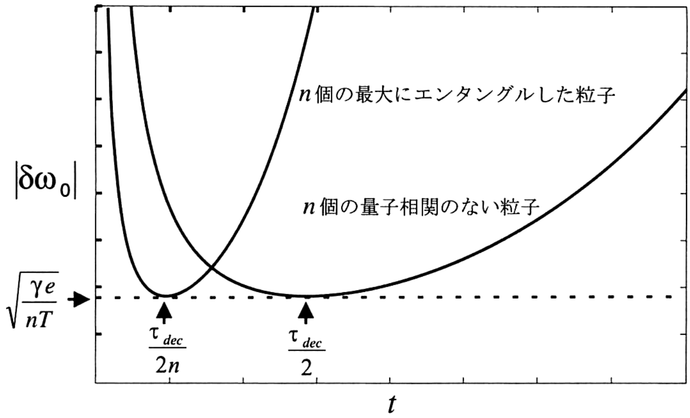


図 7.11 1 回の実験時間 t に対する周波数不確定性 $|\delta\omega_0|$．最大エンタングル状態と量子相関のない状態に対する結果を示す．最小不確定性は，両方の場合において厳密に同じ値であることに注意せよ

そして，原子周波数の推定値に対する不確定性は

$$\Delta t = \frac{k\pi}{2n} \quad (k \text{ は奇数}), \qquad\qquad t = \frac{\tau_{dec}}{2n} \tag{7.102}$$

のときに最小になる．興味深いことに，ラムゼイ分光法の結果 (7.100) とまったく同じ最小不確定性が得られる．この効果は，図 7.11 に示されている．図 7.11 は，周波数不確定性 $|\delta\omega_0|$ の t 依存性であり，n 個の量子相関のないイオンを用いた場合（ラムゼイ分光法）の結果と n 個の最大エンタングル状態を用いた場合の結果が示されている．

デコヒーレンスが存在する場合，どちらの方法を用いても同じ精度しか達成できない．この結果は，以下のように考えると直感的に理解できる．デコヒーレンスが存在する場合，最大エンタングル状態はより壊れやすくなる．そのためデコヒーレンス時間は $1/n$ に減少するので，単一測定時間 t も同じ量だけ減らす必要がある．これまでの計算結果は，全実験時間 T が典型的デコヒーレンス時間よりも長いときはいつでも成立する．そのため，最大エンタングル状態は短時間の安定化に対してのみ役に立つ．一方長時間の実験を考える場合，高い対称性をもつ部分的にエンタングルした状態を用いることによって，最大精度が達成できることが最近示された [379]．この方法は初期状

態準備および最終測定に対する最適化を必要とする．しかしながら実用的な観点からは，期待される改善はあまり大きくない．限界 (7.100) に対する最適な改善の割合は，$n = 7$ の場合 10%程度である．n が大きい場合の漸近的限界に関しては現在研究中である．

量子エンタングルメントを用いた周波数標準の精度改善のための大きく異なるアプローチは，エラー訂正を利用することである．前節で示したように，エラー訂正により量子系におけるデコヒーレンスや散逸を効果的に減少させることができる．しかしながら，位相エラーに対するエラー訂正プロトコルを適応した場合，問題が生じる．つまり，エラー訂正によって環境ノイズによる位相エラーは訂正されるが，それは（推定したい量 Δ に対応する）原子状態の望ましい相対位相変化をも妨げてしまう．これは，周波数標準の感度を下げる．にもかかわらず，後で見るようにデコヒーレンスに対して系を**安定化**させ，ラムゼイ分光法の場合に達成可能な最適精度を超えることが可能である．

その鍵は，n 個のイオン状態を自由時間発展の間対称部分空間内にとどめるということである．対称部分空間とは，n 個のイオンのヒルベルト空間の部分空間であり，その空間中にはイオンの任意の置換に対して不変な状態すべてが含まれる．n 個のイオン状態を対称部分空間内のある状態に最初に用意したとする．もし，デコヒーレンスがなければその後もその状態は常に対称部分空間内にとどまる．つまり，全系の状態を対称部分空間 [380] に射影することにより，位相エラーによる影響を部分的に取り去ることができる．$n = 2$ の場合の，この方法による不確定性の改善率を図 7.12 に示す．計算においては，まず（n 個の量子相関のないイオンを最初に用意する）ラムゼイ分光法について考えた．次に，自由時間発展の領域において対称化ステップを何度も繰り返した場合について計算した．各対称化ステップの後，対称化が成功した場合だけイオンを捨てずにとっておく．対称化が失敗した場合は，それを捨てて $|0\rangle$ にリセットし，最初からやり直す．これによって統計処理に使える実験データ数は減ってしまう．しかし図 7.12 より，この方法は実験の全体的な精度を改善する便利な戦略であることがわかる．

一般的な n およびイオンの初期状態の場合に対する，対称化法を用いて達成可能な精度の限界に関してはまだ研究中である．

対称化法は，エラー訂正法というよりむしろエラー検出法であることに注

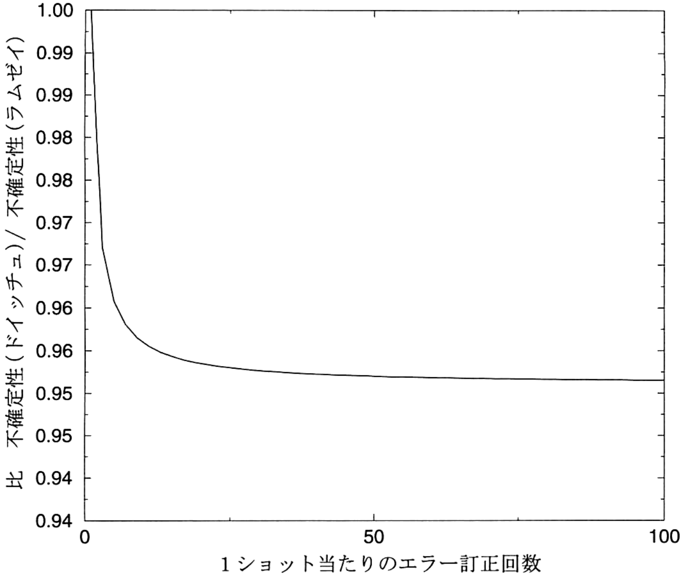


図 7.12 ラムゼイ分光法に対する，対称化法を用いた場合と用いない場合の不確定性の比．$n = 2$ の場合の結果について示す．横軸は，自由時間発展の間に行った対称化ステップの回数

意せよ．対称化法は，誤った状態を訂正する代わりに単に取り去るだけである．取り去った後に残った集合には，エラーはほとんど含まれない．しかし，対称部分空間内に残る状態数は少なくなるので，実験の統計は悪化する．そのため，全体としてはわずかに改善されるだけである．周波数標準に対する量子エラー訂正符号の適応に関しては，現在研究中である．この方向の発展によって，もしかすると実際の周波数標準の改善が行われるかもしれない．しかし，量子エラー訂正とエンタングルメントは周波数標準精度を著しく改善できないということが証明されたとしても，大変興味深いであろう．

この節においては，周波数標準におけるエンタングルメントと量子エラー訂正の応用について紹介した．この動機は，それがわずかな量子的リソースしか必要としない量子情報理論の応用だからである．量子情報理論における将来の研究の一つの方向は，きっと少ないリソースしか必要としない別の種類の応用の発展である．そのような応用は，近い将来実験的に実現されるであろう．

第8章

エンタングルメント精製

8.1 はじめに

第7章では量子エラー訂正の理論を紹介した．この章では，デコヒーレンスを克服するもう一つの方法を紹介するのだが，それは量子状態の通信において特に有効である．エンタングルメントの純度がデコヒーレンスによって低下している可能性があるエンタングルした粒子（対）の大きな集合から，エンタングルメントの純度が高められた粒子の部分集合を精製する，というのが中心的なアイディアとなる．エンタングルメント精製の一般的な原理を8.2節で説明する．具体例として，純粋状態のエンタングルメントを増加させるのに適している局所的フィルタリング（8.3節）と，雑音を含む量子通信路を用いた量子暗号の安全性を上げるために設計された量子秘匿性増幅（8.4節）が挙げられる．エンタングルメント精製の多粒子エンタングルメントへの一般化を8.5節で扱う．8.6節では，それぞれが高Q値光共振器内にあって，互いに遠く離れた原子どうしを，標準的な光ファイバのような雑音を含む通信路を通して光子を送ることによって，最大にエンタングルしたEPRペアにする方法を示す．伝送中の光子の吸収確率が距離とともに指数関数的に増加するため，伝送を成功させるために必要な繰り返しの回数も同様に増加することになる．8.7節では，量子中継器の方法を紹介する．その方法を用いると，伝送距離の関数として表される必要な操作回数の増加を，指数関数的ではなく多項式程度に抑えることが可能となる．

8.2　エンタングルメント精製の原理

(*H.-J. Briegel*)

量子通信における主な課題は，地点A（アリス）から他の地点B（ボブ）へ，雑音を含む通信路を通して量子情報を忠実に伝送することである．雑音を含む量子通信路を通して量子状態を伝送すると，一般に，その忠実度は伝送距離とともに指数関数的に減少するため，非常に短い距離しか忠実な伝送を行えないことになる．原理的には，この問題はテレポーテーションという方法を用いることによって解決される．テレポーテーションでは，最大にエンタングルした状態の粒子対（EPRペア）をAとBがいくらか共有している必要がある．そこで，もしAとBが雑音を含む通信路でしか通信できないとすると，どのようにしてAとBの間にそのようなエンタングルした状態を作り出すのか，という問題が残る．局所的操作だけではエンタングルメントを作ることができないため，非局所的な量子相関を作るためには，AとBはある時点でその通信路を通して量子ビットを送信する必要がある．これらの量子ビットは通信路と相互作用するため，デコヒーレンスは免れられず，結果として得られるEPRペアはもはや最大にエンタングルした状態ではなく，その代わりに，あるエンタングルメント忠実度をもった混合状態として記述されることになる．**エンタングルメントの精製**のアイディアとは，そのような低い忠実度のEPRペアをたくさん含むアンサンブルから，十分に高い忠実度をもった，より小さな部分アンサンブルを取り出すことであり，これらのペアは忠実なテレポーテーション [49,74]（第3章）や量子暗号 [46,47]（第2章）に利用することができる．

量子通信の観点からは，エンタングルメント精製と量子エラー訂正の間には自然なつながりがある．量子エラー訂正の理論は本来，デコヒーレンスや不完全な装置の影響のもとでも，量子計算を可能にするために考案されたのだが，もちろん，伝送エラーを訂正するために利用することもできる[1]．一方，エンタングルメント精製は量子通信のための特殊なものではあるが強力な道具である．2地点の間で古典通信を利用することにより，量子エラー訂正の方法では実現できないような，非常に効率のよい双方向通信のプロトコルが

[1] 実際，古典的なエラー訂正は，単に伝送エラーを訂正することを目的としてもともと考案された [32]．

可能となる．さらに，その方法は不完全な装置に対して著しく強いため，量子中継器 [381] のようなより進んだ応用にとっては大変魅力的なものとなっている．エンタングルメント精製と量子エラー訂正の関係の定量的な解析は参考文献 [323] で与えられている．

今日考えているような通信への特定の応用に限らず，エンタングルメントを精製すること（および，定量化すること）は基礎的な意味で興味深い問題であることを強調しておくべきだろう．将来においては，現在知っている以上に,（多）粒子エンタングルメントのより多くの側面についての理解が得られるであろうし，その応用は計算や通信だけに限定されていないかもしれない．とにかく，エンタングルした状態を実験室で実現するのはすばらしいことであり，そのためには，エンタングルした状態を発生させて，それらを効率よく精製する方法についての知識が必要となる．

それでは，エンタングルメント精製とはなんだろうか？

主な考え方を説明するために，まずはじめに，ある方向（たとえば z 方向）に部分的に偏極したスピン 1/2 粒子のアンサンブルを考えよう．話を簡単にするために

$$\rho = f|\uparrow\rangle\langle\uparrow| + (1-f)|\downarrow\rangle\langle\downarrow| \tag{8.1}$$

という密度行列で表されるような，それぞれ $|\uparrow\rangle \equiv |$ スピン上向き $\rangle$ や $|\downarrow\rangle \equiv |$ スピン下向き $\rangle$ という状態にある粒子がインコヒーレントに混合した状態を扱うことにするが，この制限は以下の議論において本質的なものではない．たとえば，図 8.1 にあるようなシュテルン－ゲルラッハ (Stern-Gerlach: SG) 装置に粒子を通して，その粒子の z 軸に沿ったスピンを測定することよって，$|\uparrow\rangle$ 状態にある粒子の部分アンサンブルを選び出すことは容易にできる．上の経路に沿って装置から出てきた粒子のみを選び出すことにより（平均すると，全体の中で割合 f の粒子がそうなる），純粋状態 $\rho' = |\uparrow\rangle\langle\uparrow|$ にある粒子の部分アンサンブルを作り出すことは確かにできる．この言い方は今の時点では多少無理があるが，望みの方向に偏極した粒子を「抽出」することにより，全体のアンサンブルを「精製」したといえるだろう．

理由は後で明らかになるが，もう少し複雑な次のような状況を考えてみよう．ある未知の仕組みにより，SG 装置を通り抜けた粒子は破壊される（たとえば，吸収される）とする！　装置は最終的にはすべての粒子を吸収する

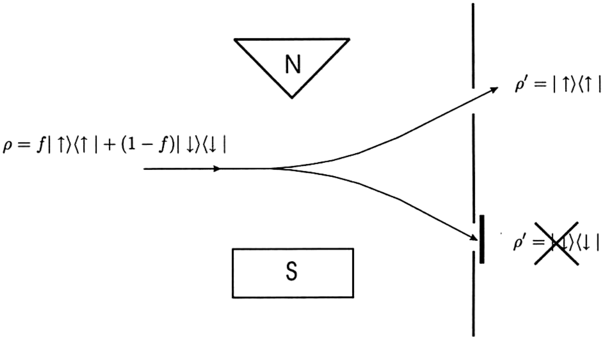


図 8.1　シュテルン－ゲルラッハ磁石を用いた，スピン偏極原子の選別：二つの磁石（S と N）によって作られた z 方向の不均一磁場を用いて，異なるスピンの粒子を空間的に分離する．この装置を簡略に，「シュテルン－ゲルラッハ装置」と呼ぶことにする

のだが，もしも粒子が図 8.1 の上の穴を通れば装置はカチッという音を出し，そうでなければ何もしないとする．どうすればこのような欠陥のある装置を使ってアンサンブルを精製できるだろうか？　一つの可能性としては，粒子それ自体ではなく，代わりにそれらのコピーを SG 装置に送るという方法が考えられる．一般の量子状態をコピーするのは不可能だが（複製不可能定理，2.2.2 項 [88]），補助粒子 C と**測定ゲート**（または，CNOT ゲート）を用いて，選ばれた**基底**の状態をコピーすることは可能である．測定ゲートについては 1.6 節に解説してある：もし粒子 C の初期状態が $|\uparrow\rangle_C$ ならば，そのゲートは粒子 A の基底の状態 $|\uparrow\rangle_A$ または $|\downarrow\rangle_A$ を粒子 C にコピーする，という作用をする[2, 3]．

$$\begin{aligned} |\uparrow\rangle_A|\uparrow\rangle_C &\longrightarrow |\uparrow\rangle_A|\uparrow\rangle_C, \\ |\downarrow\rangle_A|\uparrow\rangle_C &\longrightarrow |\downarrow\rangle_A|\downarrow\rangle_C. \end{aligned} \tag{8.2}$$

[2] このことから，このゲートによって任意の重ね合わせ $(\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)$ は次のように変換されることがわかる：

$$\begin{aligned} (\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)|\uparrow\rangle_C &\to \alpha|\uparrow\uparrow\rangle_{AC} + \beta|\downarrow\downarrow\rangle_{AC} \\ &\neq (\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)(\alpha|\uparrow\rangle_C + \beta|\downarrow\rangle_C) \end{aligned}$$

したがって，複製不可能定理 [88] には抵触しない．

[3] より一般的には，粒子 A が $|\downarrow\rangle_A$ 状態にあれば，粒子 C のスピンは反転する．すなわち，変換 $|\uparrow\rangle_A|\downarrow\rangle_C \longrightarrow |\uparrow\rangle_A|\downarrow\rangle_C$ と $|\downarrow\rangle_A|\downarrow\rangle_C \longrightarrow |\downarrow\rangle_A|\uparrow\rangle_C$ を式 (8.2) に加えることによって，CNOT ゲートは完全に記述される．

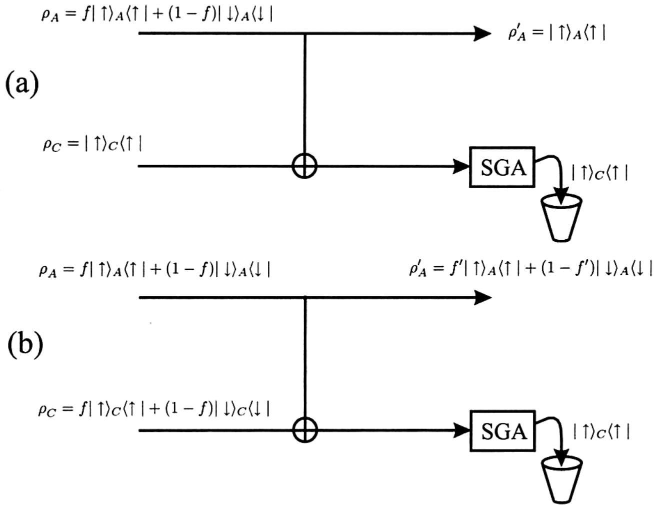


図 8.2 原子の状態を測定するとその原子を吸収してしまうような，仮想的なシュテルン-ゲルラッハ (SG) 装置を用いたスピン偏極原子の選別．混合アンサンブルの原子の状態（上の線）が補助原子 C（下の線）にコピーされて（記号 $\oplus$），その補助原子に破壊測定がなされる．(a) で用いられる補助原子は状態 $|\uparrow\rangle_C$ に偏極していて，(b) では補助原子は混合アンサンブル自体から取り出したものである

測定ゲートをアンサンブル (8.1) に適用すると，

$$\rho_{AC} = f|\uparrow\rangle_A\langle\uparrow|\otimes|\uparrow\rangle_C\langle\uparrow| + (1-f)|\downarrow\rangle_A\langle\downarrow|\otimes|\downarrow\rangle_C\langle\downarrow| \tag{8.3}$$

という形で表されるような（古典的に）相関した二つのアンサンブルが生成される[4]．もしここで補助粒子のスピンを測定したとすると，その粒子はやはり破壊されてしまうが，残された対応する粒子 A が純粋状態 $\rho'_A = |\uparrow\rangle_A\langle\uparrow|$ にあることが，カチッという音によってわかるだろう（図 8.2(a) 参照）．すべての粒子のコピーを測定することにより，どの粒子が望みどおりの状態にあるのかを確かめて，その結果，精製された部分アンサンブルを選び出すことができる．

[4] 補助粒子 C がはじめに $|\uparrow\rangle_c$ 状態にあれば，これは成り立つ．

明らかに，上の議論には落とし穴がある：**純粋状態** $|\uparrow\rangle_C$ にある補助粒子を利用できると仮定することにより，精製という考え方自体が意味のないものになってしまう．なぜなら，混合アンサンブルの代わりに，純粋状態にある補助粒子を最初から使えたはずだからである．

それでは，もしもコピーのための完全に偏極したスピンがなかったとすると，どうすればいいのだろうか？　混合アンサンブル自体から取り出した粒子を，この目的のために使うことができるというのが重要な点である．$f > 1/2$ である限りは，(コピーのために) 任意に選んだある粒子が望みどおりの内部状態 $|\uparrow\rangle_C$ にあって，アンサンブル中の他の粒子の未知の状態を確かめるために使える可能性が高い．このことを定量的に見るために，これから精製しようとしている初期アンサンブルを，同じ大きさの ρ_A と ρ_C という二つの部分アンサンブルに分けてみよう（測定ゲートにおける役割を区別するために，A と C という二つの異なる添え字をつけることにする）．どちらの部分アンサンブルも同じ密度行列 (8.1) で表される．図 8.2(b) も参照せよ．まずアンサンブル A にある各原子に対してアンサンブル C から原子を一つ選び，測定ゲートを用いて A の状態を C にコピーする．すべての粒子に対してこの手続きを行うことにより，次のアンサンブルを得る．

$$\begin{aligned}\rho_{AC} = &\,(f^2|\uparrow\rangle_A\langle\uparrow| + (1-f)^2|\downarrow\rangle_A\langle\downarrow|)\otimes|\uparrow\rangle_C\langle\uparrow| \\ &+ f(1-f)(|\uparrow\rangle_A\langle\uparrow| + |\downarrow\rangle_A\langle\downarrow|)\otimes|\downarrow\rangle_C\langle\downarrow|\end{aligned} \tag{8.4}$$

ここで粒子 C の状態を測定して，$|\uparrow\rangle_C$ 状態になった（カチッという音のした）粒子がコピーであるようなアンサンブル A の粒子をすべて集めて，新しいアンサンブルを作る．そうすると，この新しいアンサンブルは次の密度行列で表される．

$$\rho'_A = f'|\uparrow\rangle_A\langle\uparrow| + (1-f')|\downarrow\rangle_A\langle\downarrow| \tag{8.5}$$

ここで，$f' = f^2/(f^2 + (1-f)^2)$ とする．この単純な関数 $f'(f)$ は，エンタングルした混合状態の精製の議論で用いる図 8.4 のグラフの関数と同じものである．したがって，$f > 1/2$ ならば，$|\uparrow\rangle_A$ 状態にある粒子の割合がより大きな値 $f' > f$ で表されるような**精製されたアンサンブル**が得られる．初期アンサンブルが十分多くの粒子を含んでいる限りは，図 8.4 で階段状に表されているように，この手続きを繰り返すことによって，純粋状態 $|\uparrow\rangle_A$ にいくらで

も近い粒子を**抽出**することができる[5].

これでエンタングルした混合状態の精製を議論する準備が整った．異なる場所にいるアリスとボブが，それぞれ粒子 A と B を持っていて，2 粒子のエンタングルした状態 ρ_{AB} のアンサンブルを精製したいとする．次のような簡単な例を考えてみよう．

$$\rho_{AB} = f|\Phi^+\rangle_{AB}\langle\Phi^+| + (1-f)|\Psi^+\rangle_{AB}\langle\Psi^+|. \tag{8.6}$$

ここで

$$|\Phi^+\rangle_{AB} = \{|\uparrow\uparrow\rangle_{AB} + +|\downarrow\downarrow\rangle_{AB}\}/\sqrt{2}$$

と

$$|\Psi^+\rangle_{AB} = \{|\uparrow\downarrow\rangle_{AB} + +|\downarrow\uparrow\rangle_{AB}\}/\sqrt{2}$$

はベル状態を表し，また，$1/2 < f < 1$ とする．$f = 1/2$ でなければ，状態 (8.6) は分離不可能である．式 (8.6) は（純粋な）ベル状態 $|\Phi^+\rangle$ と $|\Psi^+\rangle$ の二つのアンサンブルが，それぞれ f と $(1-f)$ という割合で古典的に混ぜ合わされたものだと見なせる[6]．明らかに，アリスとボブは各粒子をそれぞれの SG 装置に通すことにより，二つの部分アンサンブルを区別することができる：アリスもボブも SG 装置を z 方向に向けているとすると，$|\Phi^+\rangle_{AB}$ 状態のペアのときには，どちらの粒子も同じ経路を通って装置から出てくるだろうし（「上－上」または「下－下」），$|\Psi^+\rangle_{AB}$ 状態のペアのときは，二つの粒子は異なる経路を通って装置から出てくるだろう（「上－下」または「下－上」）．一方，この測定により，はじめにあったエンタングルメントはすべて**破壊**されてしまい，粒子は積状態として装置から出てくるだろう．したがって，局所的な測定によってエンタングルメントを破壊してしまうのなら，アリスとボブはどうすれば $|\Phi^+\rangle_{AB}$ の部分アンサンブルを選び出せるのだろうか，ということが問題となる．

この問題を解くために，1 粒子の精製に関する以前の議論で得られた知見を利用できるかもしれない．アリスとボブは測定ゲートのからくりを使って，粒子そのものではなく，粒子 A と B の「コピー」を SG 装置へ送ることがで

[5]厳密に言えば，この方法で純粋状態を抽出するためには，はじめのアンサンブルが無限に大きなものでなくてはならない．

[6]式 (8.6) における割合 $f = {}_{AB}\langle\Phi^+|\rho_{AB}|\Phi^+\rangle_{AB}$ は，ベル状態 $|\Phi^+\rangle$ に対する混合状態 ρ_{AB} の「エンタングルメント忠実度」（または単に，忠実度）とも呼ばれる．

きるだろうか？　実際，コピーに使う粒子の初期状態自体がエンタングルしていれば，それは可能である．これが実際に可能であることを見るために，アンサンブル (8.6) の中のペア AB と，純粋状態 $|\Phi^+\rangle_{A'B'}$ にあるもう一つのペア A′B′ の二つのペアをアリスとボブが共有している状況を考えてみよう．まず，式 (8.2) で表される測定ゲートを両側で，A と A′ の間，および B と B′ の間にそれぞれ適用することにより，AB ペアの状態を A′B′ ペアにコピーする．この操作の結果は以下のようにまとめられる：

$$
\begin{aligned}
|\Phi^+\rangle_{AB}|\Psi^+\rangle_{A'B'} &\longrightarrow |\Phi^+\rangle_{AB}|\Phi^+\rangle_{A'B'}, \\
|\Psi^+\rangle_{AB}|\Phi^+\rangle_{A'B'} &\longrightarrow |\Psi^+\rangle_{AB}|\Psi^+\rangle_{A'B'}
\end{aligned}
\tag{8.7}
$$

この両側での (CNOT) 操作は，明らかにペアに対する測定ゲートのように振る舞い，$|\Phi^+\rangle$ と $|\Psi^+\rangle$ が式 (8.2) における $|\uparrow\rangle$ と $|\downarrow\rangle$ に対応する役割を果たしている．このことから，もしアリスとボブが状態 $|\Phi^+\rangle_{A'B'}$ のペアを共有していたら，アンサンブル (8.6) から任意に選んできたペアの状態を確かめるためにそれらを使うことができるため，望みの部分アンサンブルを選び出すことができることになる．もちろん，彼らが状態 $|\Phi^+\rangle_{AB}$ にある補助ペアを持っていないということが問題になるのだが！（もし持っていたら，精製する必要がなくなってしまう.）しかし，1 粒子の精製に関する以前の議論を思い出してみると，混合アンサンブル中のペアの大部分が望みの初期状態 $|\Phi^+\rangle$ にあるならば（つまり，$f > 1/2$），アリスとボブはそのアンサンブル自体に含まれるペアを同じように使ってもよさそうだ．そうすると，プロトコルは 1 粒子の精製プロトコルに大変似たものになる（図 8.3 参照）：

1. アリスとボブはアンサンブル (8.6) から二つのペアを任意に選び出して，

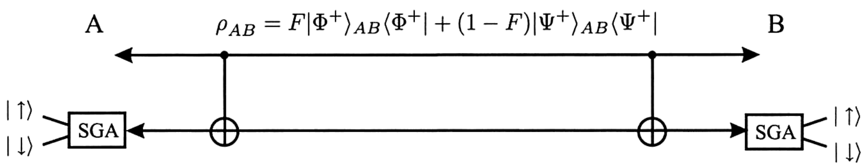


図 8.3　局所的ユニタリ変換，測定，および古典通信を用いた，エンタングルした状態の混合アンサンブルの精製

そのうちの一方のペアを，もう一方のペアの状態を測定するために用いる．すなわち，

2. 両側で，対応する粒子の間に CNOT ゲートを適用する．
3. たとえば，図 8.3 にあるように二つの SG 装置を用いて，補助ペアの状態を測定する（それにより，そのペアのエンタングルメントは破壊される）．

スピンの測定結果が同じ（上－上または下－下）だったペアのみを取っておくことによって，

$$\rho'_{AB} = f'|\Phi^+\rangle_{AB}\langle\Phi^+| + (1-f')|\Psi^+\rangle_{AB}\langle\Psi^+| \tag{8.8}$$

という密度行列で表される新しいアンサンブルを選び出すことができる．ここで，$|\Phi^+\rangle_{AB}$ 状態の割合はより大きくなって，$f' = f^2/(f^2+(1-f)^2) > f$（$f > 1/2$ のとき）となっている（図 8.4 参照）．アリスとボブは互いの測定結果を比較することによって，どのペアを取っておいて，どのペアを捨てるのかを決めるために，通信によって古典情報を交換しなければならないことに注意せよ．この古典通信はあらゆる精製プロトコルにおいて不可欠の部分である．アリスとボブは，図 8.4 で階段状に表されているように，この手続きを繰り返すことによって，エンタングルメント忠実度 f がいくらでも 1 に近いペアのアンサンブルを**抽出**することができる．

式 (8.6) を用いて，2 粒子の混合状態のかなり特殊な例について議論してきたように思えるが，十分大きな割合 $f = \langle\Phi_{me}|\rho_{AB}|\Phi_{me}\rangle > 1/2$ で，ある最大にエンタングルした状態 $|\Phi_{me}\rangle$ を含んでさえいれば，一般の状態 ρ_{AB} に対しても，この方法はうまくいく[7]．一般のエンタングルした混合状態についての最初のエンタングルメント精製プロトコルは，Bennett らによって提案された [49]．その方法を用いると，忠実度が $f > 1/2$ であるエンタングルした状態の大きなアンサンブルから，忠実度 f がいくらでも 1 に近いペアの，より小さなアンサンブルを抽出することができる．これらのペアは，雑音を含む量子通信路を通して忠実なテレポーテーションを行うために使うことができる．「量子秘匿性増幅」(QPA) と呼ばれる 2 番めのプロトコルは Deutsch らに

[7] アリスとボブの粒子に局所的なユニタリ変換を行うことによって，四つのベル状態のうちの一つに（したがって，すべてのベル状態に）なるような任意の状態を，$|\Phi_{me}\rangle$ によって表す．通常は，一般の混合状態 ρ_{AB} を扱うプロトコルの中のある時点で，両側での CNOT 操作を行う前に，ρ_{AB} の主要な成分である $|\Phi_{me}\rangle$ をベル状態 $|\Phi^+\rangle$ に変換する．

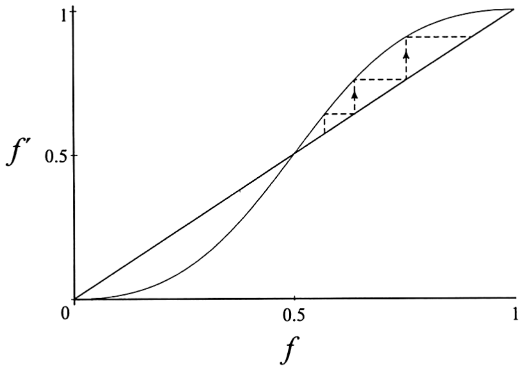


図 8.4　エンタングルした混合状態の精製．$f > 1/2$ ならば，ペア (8.6) の忠実度は，式 (8.8) の値 f' まで増加する．(階段状に) 繰り返すことにより，低い忠実度のペアをたくさん含んだ初期アンサンブルから，高い忠実度のペアを抽出することができる．この簡単な方法 (いわゆる，繰り返し法) では，各段階において全ペアの 50%以上が犠牲になることに注意せよ

よって提案された [47]．細かい点での違いを別にすれば（1 重項の精製効率など），どちらのプロトコルにおいても，エンタングルメントを破壊せずに非局所的なエンタングルした状態を測定するための主な構成要素として測定ゲートを用いる．QPA は，エンタングルメントに基づいた量子暗号 [46] への応用に主に動機づけられている．それを用いると，アリスとボブは，選び出したペアの部分集合と潜んでいる可能性のある盗聴者との間の**エンタングルメントを切る**ことが原理的にできるようになるため，あとでそれらのペアを量子鍵分配に使えるようになる．この量子秘匿性増幅の方法は 8.4 節で解説する．

エンタングルメント精製の考え方を説明してきたが，エンタングルした状態を精製する方法はこれらだけではないことを強調しておくべきだろう．プロトコルの効率を上げるために，ランダムハッシュ法 [49,323] のような古典情報理論からのアイディアを用いた，もっと精巧な（たとえば，多粒子測定を用いた）方法も存在する．おもしろくてしかも簡単な別の方法としては**局所的フィルタリング** [117,382] があり，これは**純粋**状態のエンタングルメントを増加させるのに特に適している．これについては 8.3 節でさらに詳しく解説する．数年前にはじめのアイディアが考案されてから，エンタングルメント精製の理論はさらに一連の発展を遂げてきている．この初歩的な入門ではそれ

らを取り上げることはできないが，重要な概念である「束縛されたエンタングルメント」[383] や，最適な精製プロトコルに関する議論 [322,323,384,385]，不完全な局所的操作のもとでの精製プロトコルの効率や強さ [381,386,387] などが例として挙げられる．エンタングルメント精製を，多粒子のエンタングルした状態へ一般化することについては，8.5 節で議論する．

8.3 局所的フィルタリング

(*B. Huttner, N. Gisin*)

エンタングルメント精製では，すべてが（おそらく混合状態である）同じ状態 $\rho_{\rm in}$ にあるような量子系の無限個のペアを考える．局所的操作と古典通信のみを用いて，これらのペアから最大にエンタングルした純粋状態を取り出すことが目的である．はじめに，二つの量子系がエンタングルした純粋状態 $|\psi_{\rm in}\rangle\langle\psi_{\rm in}|$ を考える．局所的フィルタリングによって，この純粋状態を 2 量子ビットの 1 重項状態 $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ へ，いつでも「精製」できることを以下で示す．この議論により，エンタングルメント精製の特に簡単な例である局所的フィルタリングの概念を紹介して，一般のエンタングルメント精製においては，1 重項状態への精製を考えれば十分であることを示す [382]．

Schmidt 分解を用いると，$\psi_{\rm in}$ はいつでも次の形に書ける：

$$\psi_{\rm in} = \sum_{j=1}^{N} c_j \alpha_j \otimes \beta_j \tag{8.9}$$

ここで，$\{\alpha_j\}$ と $\{\beta_j\}$ はエンタングルした二つの量子系のヒルベルト空間における正規直交基底を表す．状態 $\psi_{\rm in}$ がエンタングルしていると仮定したことにより，少なくとも二つの 0 でない係数 c_j が存在するため，$c_1 \neq 0$ および $c_2 \neq 0$ と仮定してよい．状態 α_j の系を持っているアリスと，β_j を持っているボブは，$\psi_{\rm in}$ を精製するために射影子 $P_{\alpha_1} + P_{\alpha_2}$ と $P_{\beta_1} + P_{\beta_2}$ をそれぞれはじめに観測する．古典通信を用いて結果を伝え合うことによって，アリスとボブは測定結果が成功と出たペアのみを取っておくことにする．これらのペアは次のような状態になる：

$$\psi_1 = c_1 \alpha_1 \otimes \beta_1 + c_2 \alpha_2 \otimes \beta_2 \tag{8.10}$$

したがって，各部分系は量子ビットのように二つの直交状態のみを含むことになる．$|c_1|^2 \geq |c_2|^2$ と仮定することにして，α_1 と β_1 を弱めるが α_2 と β_2 はそのまま通過させるような二つのフィルタ F_A と F_B を，アリスとボブは局所的に適用する．これらのフィルタは次のような正値演算子で表される：

$$F_A = \sqrt{\frac{|c_2|}{|c_1|}}P_{\alpha_1} + P_{\alpha_2} \quad \text{および} \quad F_B = \sqrt{\frac{|c_2|}{|c_1|}}P_{\beta_1} + P_{\beta_2} \tag{8.11}$$

古典通信路で結果を伝え合うことにより，アリスとボブは両方のフィルタを通過した系のペアのみを選び出す（実際には，アリスかボブのどちらかが自分の演算子を観測して，フィルタの役割を果たせば十分である）．そういうフィルタが実際に存在することに注意しよう．たとえば，偏光に依存した損失のある光学素子が一般的なものとしてあげられる．量子光学における実験例については，たとえば [388] を参照せよ．フィルタにかけられた系の状態は，両方の積状態に等しい重みをもっている：

$$\psi_2 = F_A \otimes F_B \psi_1 = \frac{|c_2|}{|c_1|}c_1\alpha_1 \otimes \beta_1 + c_2\alpha_2 \otimes \beta_2 \tag{8.12}$$

最終的には，アリスとボブは $\alpha_1 \otimes \beta_1$ と $\alpha_2 \otimes \beta_2$ の間の相対位相さえ調整すれば，（重要でない大局的位相を除いて）所望の 1 重項状態が得られる：

$$\psi_{\text{filtered}} = \alpha_1 \otimes \beta_1 - \alpha_2 \otimes \beta_2 \tag{8.13}$$

最も一般化された状況では，エンタングルメント精製の問題はさらに複雑になる（三つ以上の系がエンタングルしている場合においては，一般的な解は知られていない）．しかし，これから示すように，上述の比較的単純なフィルタを用いて精製できる混合状態もある．上記の例をヒントにして，次のような 2 量子ビットの混合状態を考えよう：

$$\rho_{\text{in}}(\lambda, c) = \lambda P_{\psi_c} + \frac{1-\lambda}{2}(P_{\psi_{11}} + P_{\psi_{00}}) \tag{8.14}$$

ここで，λ と c はともに 0 と 1 の間の実数であり，さらに

$$\psi_c = c|10\rangle - \sqrt{1-c^2}|01\rangle, \quad \psi_{11} = |11\rangle, \quad \psi_{00} = |00\rangle \tag{8.15}$$

とする．状態 $\rho(\lambda, c)$ がどのように精製されるのかを示す前に，この状態は決して Bell-CHSH 不等式を破らないことを示そう [12]．それには，Horodecki 一

家による強力な結果 [389] を用いるのだが，それを状態 $\rho(\lambda, c)$ に適用すると，

$$\frac{1}{2-2c\sqrt{1-c^2}} < \lambda \leq \frac{1}{1+c^2(1-c^2)} \tag{8.16}$$

ならば，Bell-CHSH 不等式は破られないことがわかる．したがって，$\rho(\lambda, c)$ は明らかに局所的ということになるが，以下に示すように，$\rho(\lambda, c)$ は 1 重項状態へ精製できるので，結果的に，$\rho(\lambda, c)$ は実際には非局所的だということになる．

$\rho(\lambda, c)$ を精製する過程は上で述べた例に実際にかなり似ている．アリスとボブはフィルタ (8.11) において $c_1 = c$ および $c_2 = \sqrt{1-c^2}$ と置いたものを適用する．フィルタをかけた状態は

$$\begin{aligned}\rho_{\mathrm{filtered}}(\lambda, c) &= F_A \otimes F_B \rho_{\mathrm{in}}(\lambda, c) F_A \otimes F_B \\ &= \frac{1}{N}\left(2\lambda c\sqrt{1-c^2} P_{\mathrm{singlet}} + \frac{1-\lambda}{2}(P_{\psi_{11}} + P_{\psi_{00}})\right)\end{aligned} \tag{8.17}$$

となる．ここで，$N = 2\lambda c\sqrt{1-c^2} + (1-\lambda)$ は規格化因子である．

Horodecki の定理 [389] を再び用いると，

$$\lambda > \frac{1}{1+2c\sqrt{1-c^2}(\sqrt{2}-1)} \tag{8.18}$$

のとき，およびそのときに限り，この状態は Bell-CHSH 不等式を破ることがわかる．条件 (8.16) および (8.18) によって定義される λ の上限と下限は $c\sqrt{1-c^2} \leq \sqrt{2}-1$ である限り矛盾しない．したがって，Bell-CHSH 不等式を破らないという意味において状態 $\rho(\lambda, c)$ は「局所的」であるが，局所的な環境によるフィルタにその状態を通すことによって得られる状態 $\rho_{\mathrm{filtered}}(\lambda, c)$ は，ある Bell-CHSH 不等式を破るような λ と c の値が存在する．

上記において，「局所的」≈ 「Bell-CHSH 不等式を破らない」という同一視をした．こうすることによって，結果がいくらか劇的に見えてくるのである！　しかし，明らかにこの同一視は批判を受けうるし，また受けるべきだろう．ある局所的な相互作用を受けた後に明らかに非局所的になるような状態は，局所的であるとされる資格はない．式 (8.16) および式 (8.18) を満たす状態 $\rho(\alpha, \lambda)$ が，あらゆる相関を再現するような局所的な隠れた変数モデルを許すかどうかは未解決問題の一つである．その状態は Bell-CHSH 不等式を破

らないので，そのようなモデルが存在してもよさそうだ．しかし，たとえそのような局所的な隠れた変数モデルが存在しても，その状態は非局所的と呼ばれるべきである．なぜなら，上に挙げた例で説明したように，あらゆる相関を再現するだけでは十分ではないからである．

8.4　量子秘匿性増幅

(*C. Macchiavello*)

エンタングルメント精製の目的は，純粋状態ではないエンタングルした状態の大きな集合から，純度の高められた状態の部分集合を抽出することにある．この種の方法の最初の提案は [49] でなされ，それを用いれば雑音を含む通信路を通して量子状態を忠実にテレポーテーションすることができるということが示された．その次に，さらに効率のよい精製方法が [47] において提案された．それは暗号に適用することを目的として設計されたので,「量子秘匿性増幅」(QPA) と呼ばれる．実際，雑音を含む通信路を用いた量子暗号の安全性が,（2 章でも紹介したエンタングルメントに基づいた方法 [46] においては）その方法によって得られることが証明された．この節では，QPA の方法がどのように機能するのかを説明する．

最大にエンタングルした状態の量子ビットのペアが生成されて，アリスとボブという二人のユーザへ，雑音を含む通信路を通して分配されたとしよう．伝送路における雑音のために，分配されたペアは，相互作用によって環境とエンタングルして純度を失い，そして混合状態になってしまう．アリスとボブは受け取ったペアを操作することによって，それらのペアの純度を上げたいと考えている．ペアはたくさん配られて，通信路はすべてのペアに対して同様に作用すると仮定しよう．ペアの状態をベル基底表現

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{8.19}$$

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{8.20}$$

を用いて表すことにする．ここで，$\{|0\rangle, |1\rangle\}$ はペアの各粒子の基底を表す．各ペアは，はじめは状態 $|\phi^+\rangle$ に生成されるとして，アリスとボブが受け取る

「雑音の影響を受けた」ペアの密度演算子 ρ の，基底 $\{|\phi^+\rangle, |\psi^-\rangle, |\psi^+\rangle, |\phi^-\rangle\}$ における対角要素を $\{a, b, c, d\}$ で表す．一つめの対角要素 $a = \langle\phi^+|\hat{\rho}|\phi^+\rangle$ は「忠実度」と呼ばれていて，そのペアが $|\phi^+\rangle$ という状態にあるかどうかのテストを通過する確率を表す．QPA の目的は忠実度を 1 にもっていくことである（つまり，他の三つの対角要素が 0 になることを意味する）．雑音の影響を受けたペアの密度行列全体を記述する必要はないことに注意しよう．なぜなら，QPA のアルゴリズムでは平均すると（すなわち，手続きの各段階において，分配されたペアのアンサンブル全体にわたって平均を取ると），非対角要素は対角要素の時間発展に寄与しないので，この方法の効率を調べるうえでは重要ではないからである．

QPA の手続きにおいては，アリスとボブは雑音の影響を受けたペアを受け取ってから，それぞれが二つのペアを含むようなグループにそれらを分けて，各グループに対して以下のような操作を行う．アリスはユニタリ変換

$$U_A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{8.21}$$

を自分の 2 量子ビットのそれぞれに行い，ボブはその逆演算

$$U_B = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{8.22}$$

を自分のものに行う．もし量子ビットがスピン 1/2 粒子で，計算基底がそれらのスピンの z 成分の固有状態だとすると，二つの操作はそれぞれ，x 軸に関する $\pi/2$ および $-\pi/2$ 回転となる．

それから，アリスとボブは，1.6 節で説明した量子制御 NOT 演算

$$\underset{\text{制御}}{|x\rangle}\ \underset{\text{標的}}{|y\rangle} \rightarrow \underset{\text{制御}}{|x\rangle}\ \underset{\text{標的}}{|x \oplus y\rangle} \qquad (x, y) \in \{0, 1\} \tag{8.23}$$

をそれぞれ行う．ここで，一方のペアが二つの制御量子ビットになり，もう一方のペアが二つの標的量子ビットとなる．また，2 を法とする足し算を $\oplus$ で表す（この両側での制御 NOT 演算のベル基底における振る舞いを記述した有用な表が [49] にある）．それから，アリスとボブは標的量子ビットを計算基底で測定する（たとえば，標的スピンの z 成分を測定する）．測定結果

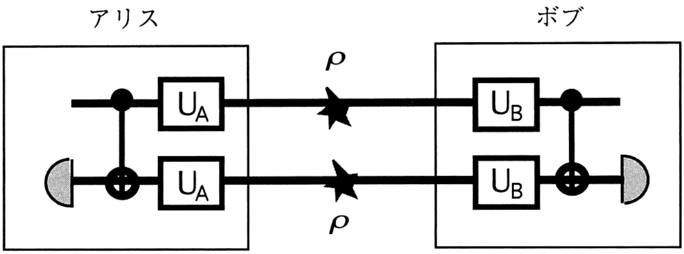


図 8.5　QPA の手順の図式表現．アリスが自分の粒子に演算 U_A と制御 NOT 演算を行い，ボブも演算 U_B と制御 NOT 演算を行う．それから，アリスとボブは標的ペアを測定して，その結果が一致した場合には，制御ペアを次の繰り返し操作のために取っておく

が一致した場合には（どちらもスピン上向きだったり，どちらもスピン下向きだった場合），制御ペアを次の回まで取っておき，標的ペアは捨てる．測定結果が一致しなかった場合には，どちらのペアも捨てる．QPA の手続きにおける基本的な操作は図 8.5 に体系的に示してある．

この手続きの結果を見るために，はじめに各ペアが $\{a, b, c, d\}$ という対角要素をもった同じ状態にあると仮定しよう．制御量子ビットが保持されている場合は，それらの密度演算子の対角要素 $\{A, B, C, D\}$ は，平均すると，対角要素 $\{a, b, c, d\}$ のみによって決まる．

$$A = \frac{a^2 + b^2}{p} \tag{8.24}$$

$$B = \frac{2cd}{p} \tag{8.25}$$

$$C = \frac{c^2 + d^2}{p} \tag{8.26}$$

$$D = \frac{2ab}{p} \tag{8.27}$$

ここで，$p = (a + b)^2 + (c + d)^2$ は，アリスとボブの標的ペアの測定において，結果が一致する確率を表す．式 (8.24)-(8.27) は QPA アルゴリズムの基本的な手順を示している．前の繰り返しにおいて生き残ったペアに，上記の基本的な手順を再び適用するということを繰り返していく．もし忠実度の平均値が 1 に到達するならば，生き残った各ペアはそれぞれ純粋状態 $|\phi^+\rangle\langle\phi^+|$ に近づかなくてはならないことに注意せよ．

ついでに触れておくと，もし二つの入力ペアがそれぞれ $\{a, b, c, d\}$ と $\{a', b', c', d'\}$ という対角要素を持った異なる密度演算子 ρ と ρ' で表される場合には，保持される制御ペアは，平均して次のような対角要素を持つことになる．

$$A = \frac{aa' + bb'}{p} \tag{8.28}$$

$$B = \frac{c'd + cd'}{p} \tag{8.29}$$

$$C = \frac{cc' + dd'}{p} \tag{8.30}$$

$$D = \frac{ab' + a'b}{p}, \tag{8.31}$$

ここで，$p = (a+b)(a'+b') + (c+d)(c'+d')$ であり，これらは式 (8.24)-(8.27) を一般化したものとなっている．

QPA 写像 (8.24)-(8.27) のいくつかのおもしろい性質を簡単に確かめることができる．たとえば，ある段階で忠実度 a が $\frac{1}{2}$ より大きければ，もう 1 回繰り返した後でも依然として $\frac{1}{2}$ を越えている．a は必ずしも繰り返し回数の関数として単調に増加するわけではないが，目標とする点である $A = 1, B = C = D = 0$ はこの写像の不動点であり，さらに，$a > \frac{1}{2}$ の領域における唯一の不動点になっている．この点が局所的アトラクタになっていること，すなわち a が 1 に近ければ $A > a$ であることは解析的に容易に確かめられる．

この点が $a > \frac{1}{2}$ の領域における大局的アトラクタでもあるということが最近，解析的に証明された [390]．その証明は，関数 $f(a, b) = (2a-1)(1-2b)$ が繰り返し回数の関数として単調であり，漸近的に 1 に近づくということの証明に基づいている．このことから，もしはじめのペアが，平均忠実度は $\frac{1}{2}$ を越えているが，それ以外の点では環境と任意の相関を持っているような任意の状態にあったとすると，繰り返し操作を引き続いて生き延びたペアの状態はいつでも忠実度 1 の純粋状態 $|\phi^+\rangle$ に収束するということがわかる．QPA の方法が，任意の初期値 $b > \frac{1}{2}$（この場合，純粋状態 $|\phi^+\rangle$ へ辿り着く）や，任意の初期値 $c > \frac{1}{2}$ または $d > \frac{1}{2}$（この場合，純粋状態 $|\psi^+\rangle$ へ辿り着く）に対して，いつでもうまくいくことも示せる [390]．それに比べて，初期密度演算子の対角要素がどれも 1/2 を越えていない場合は，この方法はうまくいかない．

QPA は，少なくとも一つの最大にエンタングルした状態（すなわち，ベル

状態もしくはベル状態に局所的ユニタリ変換を行うことによって得られる状態）に対する平均忠実度が 1/2 より大きいような任意の状態 ρ の集合を精製することができる．このことは，そのタイプの任意の状態が局所的ユニタリ変換によって，$|\phi^+\rangle$ へ変換できるという事実によっている [73]．最大にエンタングルした純粋状態（一般化されたベル状態）の集合を $\mathcal{B}$ で表すことにすると，状態 ρ が QPA を用いて精製できるための条件は

$$\max_{\phi\in\mathcal{B}}\langle\phi|\rho|\phi\rangle > \frac{1}{2} \tag{8.32}$$

となる．

この方法のスピードと収束に関する振る舞いは，初期密度演算子の対角要素の値に依存する．例として，$a > \frac{1}{2}$ および $b = c = d$ の場合に，初期忠実度と繰り返し回数の関数としての平均忠実度を，図 8.6 にグラフで示してある．

QPA の方法は捨てられる粒子の数の点ではかなり無駄が多い．少なくとも半分の粒子（標的として使われるもの）が各繰り返し操作において失われる．しかし，この方法の効率は，[49] で示されたエンタングルメント精製のはじめの提案の効率をしのぐ（a が 0.5 に近ければ約 1000 倍効率がよい．つまり，あらかじめ決められた最終的な忠実度のある値に対しては，生き残るペアの数は 1000 倍大きい）．

8.5　精製の多粒子エンタングルメントへの一般化

(*M. Murao, M. B. Plenio, S. Popescu, V. Vedral, P. L. Knight*)

この節では，[391] で提案された直接的な精製プロトコルを，広範囲の N 粒子エンタングルメントの混合対角状態について説明する．この方法は，Bennett ら [49] や Deutsch ら [47] の 2 粒子の精製方法ほど一般的ではないが，多粒子エンタングルメントを理解する上で重要であり，実際上の重要な応用がある．スピン 1/2 粒子がたくさんある場合，最大にエンタングルした状態とは

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\cdots0\rangle \pm |11\cdots1\rangle) \tag{8.33}$$

と，局所的ユニタリ変換の範囲内でこれに等価なものである．各粒子の状態は $\{|0\rangle, |1\rangle\}$ 基底で記述される．3 粒子の場合については，これらは GHZ 状

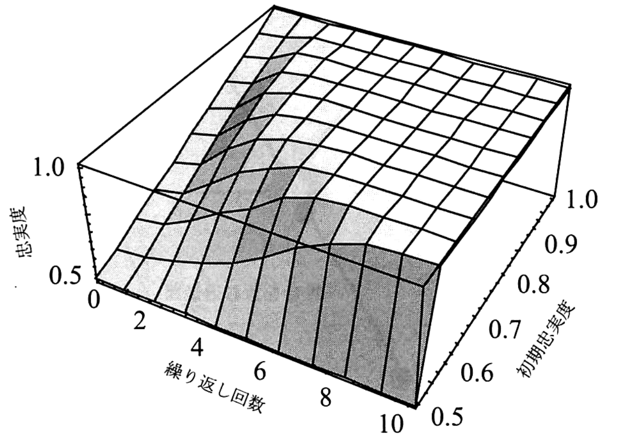


図 8.6 $b = c = d$ である初期状態の場合の，初期忠実度と繰り返し回数の関数としての平均忠実度

態と呼ばれる [290].

精製の手続き [47, 49, 117, 382] では，局所的操作と古典通信を用いて，エンタングルした**混合**状態のアンサンブルから最大にエンタングルした**純粋**状態の部分アンサンブルを「抽出」する．2 粒子の場合，1 重項状態 $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ は完全反対称なのだが，任意の両側での回転に対して不変であり，これらの精製方法において重要な役割を果たす.

しかし 3 粒子以上の場合は，3 箇所（多箇所）での回転のもとで不変になる最大にエンタングルした状態が存在しない（局所的ユニタリ変換のもとでの不変量に基づいたエンタングルした状態の分類については，[392] を参照せよ）．局所的な回転は（n を整数として，$n\pi$ の自明な回転をするのでなければ）最大にエンタングルした状態を最大にエンタングルした状態の重ね合わせに写してしまう．このことにより，**任意の**状態を Werner 状態の一つに変換するのがより難しくなってしまうため，一般的な精製プロトコルを見つけるのがあまり簡単ではなくなってしまうのである.

任意の両側での回転のもとで不変な最大にエンタングルした状態は，（N をエンタングルした粒子の数として）$N \geq 3$ の場合には存在しないが，

$$\rho_W = x|\phi^+\rangle\langle\phi^+| + \frac{1-x}{2^N}\mathbf{1} \tag{8.34}$$

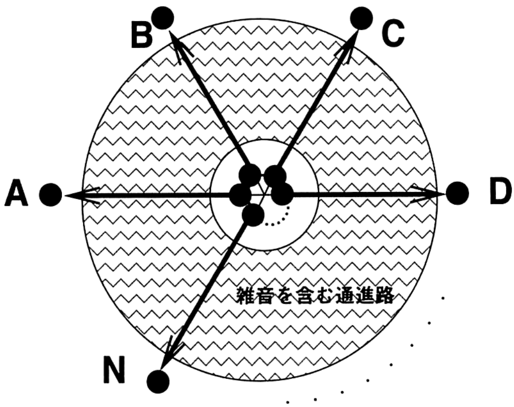


図 8.7　最大にエンタングルした状態の N 粒子を，雑音を含む通信路を通して異なる地点 (A, B, C, D,$\cdots$, N) へ伝送する

を，2 粒子の場合と似ていることから,「Werner 型状態」と呼ぶことにする．都合上，$|\psi^-\rangle$ の代わりに $|\phi^+\rangle$ と書いていることに注意せよ．精製の目的は，$|\phi^+\rangle$ 状態にある部分アンサンブルを抽出することである．この Werner 型状態の忠実度

$$f = \langle\phi^+|\rho_W|\phi^+\rangle \tag{8.35}$$

は，$f = x + (1-x)/2^N$ となる．はじめに最大にエンタングルした N 粒子状態（たとえば，$|\phi^+\rangle$）のアンサンブルがあったとして，その N 粒子を雑音を含む通信路を通して異なる N 地点へ送ると，混合状態になるであろうから，これらの Werner 型状態は実際上重要である（図 8.7）.

各粒子への作用が，任意の方向についての任意の回転で表されるような，雑音を含む通信路の効果を考えてみよう．雑音を含む各通信路は，確率 $1-x$ で（任意の方向の周りでの，任意の角度の）任意の回転を引き起こすが，確率 x で粒子に何も影響を及ぼさないものとする．そのような通信路を通して伝送された状態は，式 (8.34) で与えられるような Werner 型状態になる．

以下では，初期混合状態の忠実度がある臨界値より高ければ，Werner 型状態を精製できるようなプロトコルを紹介する（図 8.8 の P1+P2）．このプロトコルの利点は，**任意の粒子数**の Werner 型状態を**直接**に精製できる点にある．

プロトコル P1+P2 では，各地点（アリスやボブら）が，操作 P1 とそれに引き続く P2 を自分たちの粒子に繰り返し行う．

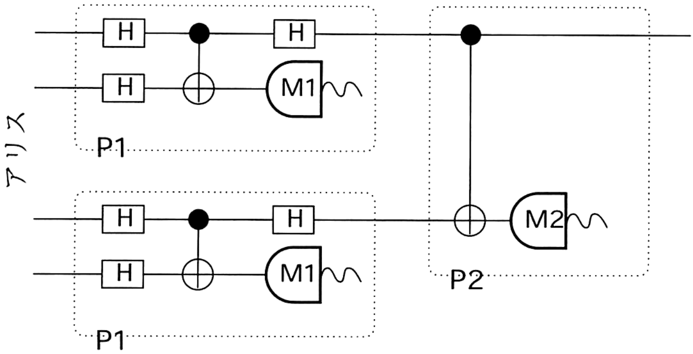


図 **8.8** 精製プロトコル P1+P2．H はアダマール変換，M1 と M2 は局所的測定と古典通信を表す．この図は，アリスのもとにある 4 粒子を表している．ボブや他の者もまったく同じ手続きを行う

- 操作 P1 は，$|0\rangle \to (|0\rangle + |1\rangle)/\sqrt{2}$，$|1\rangle \to (|0\rangle - |1\rangle)/\sqrt{2}$ という写像を行う局所的アダマール変換と，局所的 CNOT（制御 NOT）変換，さらに，測定 M1 と，再び局所的アダマール変換を行うことで構成される．測定 M1 では，偶数個の標的量子ビットが状態 $|1\rangle$ にあると観測された場合には制御量子ビットを取っておいて，そうでない場合は制御量子ビットを捨てる．たとえば 3 粒子の精製では，$|000\rangle, |011\rangle, |101\rangle, |110\rangle$ のみを取っておくことになる．
- 操作 P2 は，局所的 CNOT 変換と測定 M2 で構成されるが，その測定においては，標的ビットがすべて同じ状態にあると観測された場合に制御量子ビットを取っておいて，そうでない場合には制御量子ビットを捨てる．たとえば 3 粒子の精製では，$|000\rangle$ と $|111\rangle$ のみを取っておくことになる．この操作では，密度行列の対角要素と非対角要素は互いに独立であるため，非対角要素は精製に影響を及ぼさない．

しかし，この精製の方法は Werner 型状態のみに限られるわけではない．プロトコル P1 または P2 のみによって精製可能なタイプの状態もいくつか存在する．たとえば，もし初期混合状態が対になる状態（状態 $|\phi^-\rangle$ を $|\phi^+\rangle$ の「対になる状態」と呼ぶ）を含まなくて，さらに，他の状態の重みが等しい場合には（重みが 0 の状態がある場合でも），操作 P2 のみを繰り返し行えば，初期アンサンブルから状態 $|\phi^+\rangle$ を精製することができる（さらに詳しくは [391]

を参照せよ）.

上述の精製プロトコルでは，多粒子のエンタングルした状態が直接に精製された．これは典型的な多粒子エンタングルメントの基礎的研究には欠かせないことである．しかし，2 粒子の精製を用いて多粒子エンタングルメントを精製する方法を考えることもできる.（アリス，ボブ，クレアの）3 粒子を精製するこのような方法の一つは，2 粒子の精製方法を用いることである．この方法では，まず 3 粒子状態を 2 粒子状態へ変換して，それからこれらの 2 粒子状態を精製して，最後にそれらの状態から 3 粒子のエンタングルした状態を再構成する．言葉で説明しようとすると，このプロトコルのアルゴリズムは少し複雑になってしまうので，全体の方法を視覚的にわかりやすくするための図（図 8.9）を用いよう．その手順は以下のようになる．

1. 3 粒子状態のアンサンブル全体を，二つの等しい部分アンサンブルに分割する．
2. ボブが一方の部分アンサンブルの粒子を

$$|\chi^{\pm}\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$$

へ射影して，クレアがもう一方の部分アンサンブルを用いて，同じ射影を行う．ボブかクレアが $|\chi^{-}\rangle$ に射影することに成功したときは，彼らはアリスに自分の粒子に σ_z 変換を行うように指示する．もし彼らが $|\chi^{+}\rangle$ に射影することに成功したときは，アリスに何もしないように指示する．これら操作の最終的な結果として，2 粒子のエンタングルした状態の二つの部分アンサンブルが得られる（一方のペアはアリスとボブがもっていて，もう一方はアリスとクレアがもっている）．
3. それから，アリスとボブの組と，アリスとクレアの組はそれぞれ別々に，[47, 117] にある 2 粒子の精製プロトコルをそれぞれの 2 粒子のエンタングルした部分アンサンブルへ適用する．この結果，アリスとボブ，およびアリスとクレアの間にそれぞれ最大にエンタングルしたペアのアンサンブルができ上がる．
4. ここで，アリスは自分がボブとクレアとの間に共有している二つの最大にエンタングルした状態から，一つの GHZ 状態を取り出そうとする．そのために，アリスは各部分アンサンブルからエンタングルしたペアを一

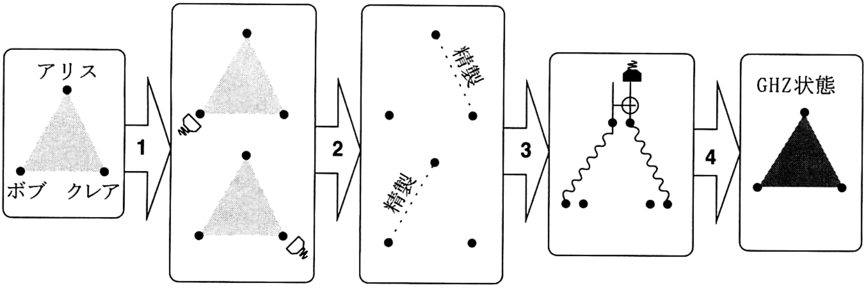


図 8.9 2粒子の精製を用いた精製方法．点線は不完全なエンタングルメントを，波線は最大のエンタングルメントを表す．（白い検出器の記号で表された）1番めの測定は，状態 $|\chi^{\pm}\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ に射影して，（黒い検出器の記号で表された）2番めの測定は，状態 $|0\rangle$ または $|1\rangle$ に射影する

つずつ選び出して，CNOT 操作を自分の2粒子に行い，それから標的粒子を $|0\rangle$ か $|1\rangle$ へ射影する．もしアリスが $|1\rangle$ へ射影するのに成功したとすると，彼女は σ_x 操作を自分の粒子に行うようにクレアに指示して，そうでないときには何もしない．そうすると，最大にエンタングルした GHZ 状態を含んだ部分アンサンブルが得られる [300, 303].

ここでこの間接的な方法を分析して，直接的な精製方法と比べてみよう．3粒子を直接精製する効率的な方法はすべて，2粒子を用いたこの間接的な方法よりうまく機能するべきである．この方法では，2粒子の最大にエンタングルした状態二つから，3粒子の最大にエンタングルした状態一つが得られるだけだということに注意しよう（図 8.10，詳しくは [391] を参照）．N 粒子のエンタングルした状態の精製では，2粒子の最大にエンタングルした状態 $N-1$ 個から，一つの最大にエンタングルした状態が得られる．さらに，2量子ビット間の CNOT 操作というのは高い精度で実行するのが実際には難しいのだが，間接的方法におけるその操作の数は直接的な方法のよりも多くなってしまう．主にこの「非効率性」が，実際上は，2粒子の方法の不利な点となる．

2粒子のエンタングルメントの場合，もし初期状態に対して何も知らなければ，精製がうまくいくためには初期忠実度が $f > 1/2$ であれば十分である [47]．もし状態に関する情報をもっと持っていれば状況は変わり，任意のエン

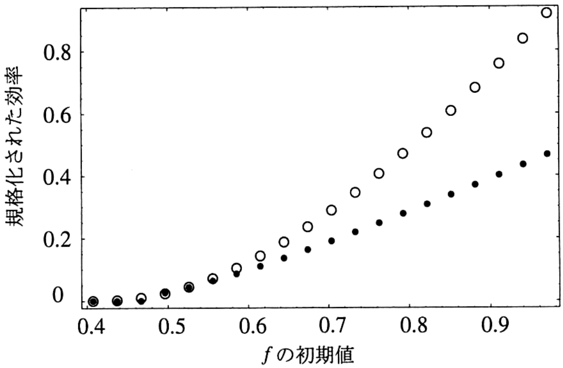


図 8.10　忠実度 f の初期値に対する，3 粒子 Werner 型状態の精製の規格化された効率．白丸は，精製プロトコル P1+P2 を用いて，精度 10^{-7} のもとでの数値計算によって得られた．黒丸は，同じ精度の 2 粒子の精製を用いた精製方法により得られた

タングルした状態を精製することができる [50]．しかし 3 粒子以上の場合には，十分条件はそんなに単純にはならない．われわれは，混合状態のタイプに依存した異なる規準をいくつか見つけた．

$\rho_W = x|\phi^+\rangle\langle\phi^+| + \frac{1-x}{2^N}\mathbf{1}$ という形の Werner 型状態をプロトコル P1+P2 で精製した場合，表 8.1 に示されているような結果が数値計算によって得られる．

2 粒子の精製を用いて Werner 型状態 ρ_W を精製した場合についての理論的な忠実度の限界は，元の状態から得られた 2 粒子状態の忠実度 f_r が $f_r > 1/2$ を満たすべきだという条件によって決定される．たとえば，3 粒子の場合に

表 8.1　A:直接的なプロトコル P1+P2 を用いて精製可能な N 粒子 Werner 型状態について，数値計算で得られた，初期状態の忠実度の限界値，B:2 粒子の精製を用いた間接的な精製方法の忠実度の理論的な限界値，C:精製するために十分な忠実度の理論的な最小値

N	A	B	C
2	$f \geq 0.5395$	$f > 1/2 = 0.5$	$f > 1/2$
3	$f \geq 0.1073$	$f > 5/12 \approx 0.4167$	未知
4	$f \geq 0.313$	$f > 3/8 = 0.375$	未知
5	$f \geq 0.245$	$f > 17/48 \approx 0.3542$	未知
6	$f \geq 0.20$	$f > 11/32 \approx 0.3438$	未知

は，初期忠実度が $f = x + (1-x)/8$ であるような Werner 状態は，ボブとクレアが測定した後に

$$\rho_r = x|\phi^+\rangle\langle\phi^+| + \frac{1-x}{4}\mathbf{1} \tag{8.36}$$

という 2 粒子状態へ変形される．

変形された 2 粒子状態の忠実度は $f_r = (1+6f)/7$ となる．4 粒子の場合は $f_r = (1+4f)/5$ となり，5 粒子の場合は $f_r = (7+24f)/31$，6 粒子の場合は $f_r = (5+16f)/21$ などとなる．表 8.1 から，プロトコル P1+P2 は 2 粒子の場合には最適ではないことがわかる．したがって，$N > 2$ の場合にも最適ではないかもしれない．しかし，3 粒子以上の場合，われわれが得た忠実度の限界は 2 粒子の精製を用いた精製方法で得られるものよりも小さくなっている．

$|\phi^-\rangle\langle\phi^-|$ を含まなくて，$|\phi^+\rangle\langle\phi^+|$ 以外の他のすべての状態に同じ重みを持つような状態に対しては，プロトコル P2 による精製の忠実度の限界は $f > 2^{-(N-1)}$ となる．2 粒子の精製を用いた精製方法による忠実度の限界は，3 粒子の場合は $2/5 = 0.4$，4 粒子の場合は $23/65 \approx 0.35846$，そして 5 粒子の場合は $125/377 \approx 0.328912$ などとなる．つまり，われわれのプロトコルより悪くなるのである．

これまで見てきたように，精製可能な初期状態の忠実度の限界は，他の対角状態の重みの分布に依存する．これは 2 粒子の場合とは異なった性質の条件である [47]．2 粒子の場合は，他の対角要素の重みの分布は精製には基本的に関係なかった．なぜなら，他の対角要素の重みの分布はどのようなものであっても，局所的な任意の回転を両方の粒子に行うことにより，エンタングルメントの量を変えることなく等しい重みの分布に変換することができるからである．このことにより，2 粒子の混合状態の場合には存在しなかったような構造が，エンタングルした多粒子の混合状態の場合には存在することが示唆される．

8.6 量子ネットワーク II：雑音を含む通信路での通信

(*H.-J Briegel, W.Dür, S.J.van Enk, J.I.Cirac, P.Zollers*)

空間的に離れた原子がそれぞれ高 Q 値光共振器の中にあるとする．標準的な光ファイバのような，雑音を含む一般的な通信路を通して光子を送ること

によって，それらの原子の間に最大にエンタングルしたEPRペアを作る方法を紹介する．各共振器の中にある二，三の補助原子を用いたエラー訂正によって，光子吸収や他の伝送エラーを効果的に減らすことができる．通信路の吸収長やコヒーレンス長よりずっと長い距離の通信を行うための，新しい入れ子状の精製プロトコルを説明する．そのプロトコルによって，古典通信における中継器と類似したものが実現される．

8.6.1　はじめに

この項では，6.2節の議論を一般化してさらに続けることにする．そこでは，量子ビットを保存しておく物理的な基礎として，原子の寿命の長い状態を用い，そしてこれらの量子ビットをある原子から他の原子へ転送する方法として，光子を用いるような量子ネットワークの実現を提案した．量子ビットの転送を制御するために，原子は光ファイバでつながれた高フィネス光共振器内に閉じ込められている（図6.1参照）．

共振器–ファイバ合成系は，レーザパルスとともに，**雑音を含む量子通信路**と抽象的に呼ばれるものを構成する（図8.11参照）．光子が光ファイバを通して送られるときの主要な転送エラーは，光子吸収によるものだろう．共振器の鏡の表面や，共振器とファイバの間の接続部分におけるインコヒーレント散乱によって引き起こされる損失もあるだろう．他の典型的な転送エラーとしては，Raman遷移のためのレーザパルスの設計が不完全であることによって引き起こされるものもある．また，局所的なゲートのエラーの例としては，ゲート操作中の原子の一つにおける自然放出が挙げられる．

この節では，散逸や雑音によるエラーのもとでも忠実度の高い通信を可能にする方法と，デコヒーレンスの影響と戦う方法を紹介する．はじめに6.2節の議論を簡単に要約することにより，エラー訂正や量子情報理論の言葉に適した表記法を導入することにする．8.6.3項および8.6.4項では，光子の転送中に起きる転送エラーに集中して，それらのエラーをどうやって見つけて訂正するのかを紹介する[393]-[395]．この議論では，局所的なゲート操作と測定はエラーなしで行えるものと仮定する．8.7節ではこの仮定をゆるめて，局所的なものも転送中のものも，すべての操作が不完全でもよいとする．このことは，エラー訂正のあらゆる方法を用いたが，何らかのエラーを見逃してしまい訂正しそびれてしまう可能性を捨て切れなかったり，もしくは，わ

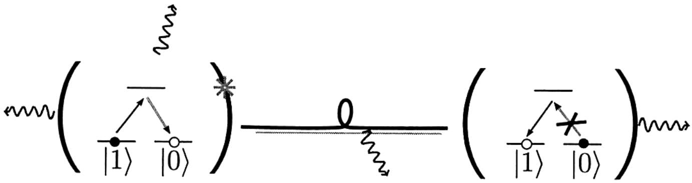


図 8.11　雑音を含む光子通信路：典型的な伝送エラーとしては，光子吸収，インコヒーレント散乱，そして，不完全な Raman 遷移が挙げられる

れわれが行う操作や測定がある意味で不正確であるというような，一般的な状況を表している．このような一般的な状況において,「長距離」通信という重要な問題と量子中継機の利用を研究する．

形式的な観点からは，量子通信とは，未知の量子ビットを通信路を通して直接送信する代わりに，通信路を通して遠距離の量子相関を作り出すことが課題であると言い換えたほうが都合がよい．ひとたび EPR ペアが作られると，情報を実際に送信するテレポーテーション [74] や，また，量子暗号 [46] の秘密鍵分配という他の目的にも用いることができる．完全な EPR ペアが作られるまでは，真の情報処理は行われていないという意味で，このアプローチは量子計算とは異なるということを指摘しておく価値はあるだろう．後で伝送に使えるような非局所的な量子相関を作り上げることがすべてとなる．実際，その後では通信路は存在する必要すらないのである．

したがって，この章の課題は，A と B をつなぐ任意の長さ l の雑音を含む量子通信路を使って，A と B の間にどうやって EPR ペアを作り出すかということになる．

8.6.2　理想的な通信

理想的には，6.2 節の方法は次の伝送を実現する．

$$[\alpha|0\rangle_A + \beta|1\rangle_A]\,|0\rangle_B \longrightarrow |0\rangle_A\,[\alpha|0\rangle_B + \beta|1\rangle_B] \tag{8.37}$$

ここで，1 番めの共振器の中にある原子 A の $|0\rangle = |e\rangle$ と $|1\rangle = |g\rangle$ という内部状態の未知の重ね合わせが，2 番めの共振器の中の原子 B へ転送される．図 8.12 を再び参照せよ．共振器は大きなネットワークの一部かもしれないので，それらをしばしばノード A，ノード B と呼ぶ．原子の選ばれた内部状態

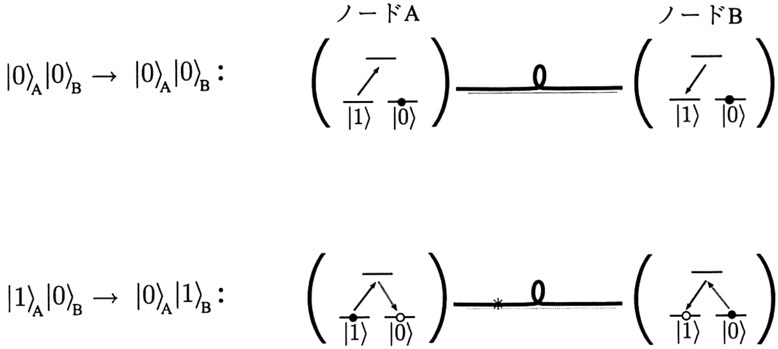


図 8.12　原子の状態をノード A とノード B の間で交換する．原子 A が状態 $|1\rangle_A$ にあるとき，その状態とノード B にある原子を光子の転送によって交換するために，6.2 節で示したような Raman 遷移の列を使うことができる．原子 A が状態 $|0\rangle_A$ にあるときは，Raman パルスは状態を変えない．そのため，状態 $|0\rangle_A$ と $|1\rangle_A$ の重ね合わせは式 (8.38) に従ってノード B へ転送される

$|0\rangle$ と $|1\rangle$ は，量子情報理論の言葉でいうところの，量子ビットの「計算基底」を定義する．

原子 A が同じ共振器内か，もしくはネットワーク上の他のノードにある他の原子とエンタングルしているかもしれないことに気がつくのは重要である．そのような状況では，式 (8.37) の係数 α と β は，もはや複素数ではなく，他の原子の規格化されていない状態を表す．したがって，式 (8.37) で表されるような送信は一つの原子状態を転送するのに使えるだけでなく，**エンタングルメント**を転送するのにも使える．たとえば，1 粒子状態から出発して，EPR ペアを 2 段階の過程

$$[\alpha|0\rangle_A + \beta|1\rangle_A]\,|0\rangle_{A_2}|0\rangle_B \longrightarrow [\alpha|0\rangle_{A_2}|0\rangle_A + \beta|1\rangle_{A_2}|1\rangle_A]\,|0\rangle_B$$
$$\longrightarrow |0\rangle_{A_2}\,[\alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|1\rangle_B] \qquad (8.38)$$

によって生成することができる．ここで，1 番めの矢印は一つめの共振器内にある二つの原子 A と A_2 の間の**局所的な** CNOT 演算を表す．2 番めの矢印は A_2 の状態を B へ転送するので，それによって，原子 A と A_2 の間のエンタングルメントを原子 A と B の間のエンタングルメントへと転送することになる．この合成変換の最後に，補助原子 A_2 の状態ははじめと同じになる

ので因数分解される．$\alpha = \beta$ ならば，理想的な EPR ペアが生成される．

8.6.3 伝送エラーの訂正：光子通信路

現実的なモデルでは，共振器 A から B への原子の状態の転送が不完全である可能性を考えなければならない．たとえ A が励起していても，B の原子が励起していないという可能性もある．これは，原子－共振器－ファイバの合成系と環境の相互作用によるものであり，たとえ小さくても，それは原理的にはいつでも存在する．この結果，式 (8.37) の原子の状態と環境，すなわち共振器の壁やファイバ，自由空間の輻射場との間のエンタングルメントが生じる．

以下では，通信路において光子は吸収はされ得るが，生成はされないものと仮定する．これは光子にとっては非常によい近似であり，そこでは，共振器とファイバの中での平均光子数は非常に少ない．この状況における不完全な転送の最も一般的な表現は，次のような形をしている．

$$\begin{aligned} |0\rangle_A|0\rangle_B|E\rangle &\longrightarrow |0\rangle_A|0\rangle_B|E_0\rangle \\ |1\rangle_A|0\rangle_B|E\rangle &\longrightarrow |0\rangle_A|1\rangle_B|E_1\rangle + |0\rangle_A|1\rangle_B|E_a\rangle \end{aligned} \tag{8.39}$$

ここで，$|E\rangle, |E_0\rangle, \cdots$ は環境の規格化されていない状態を表す．$|E_0\rangle = \mathcal{T}_0|E\rangle$, $|E_1\rangle = \mathcal{T}_1|E\rangle, |E_a\rangle = \mathcal{T}_a|E\rangle$ と書くと都合がよいので，系と環境をエンタングルさせる演算子をこれによって導入する．この表記法によると，式 (8.39) は

$$\begin{aligned} |0\rangle_A|0\rangle_B &\longrightarrow |0\rangle_A|0\rangle_B\mathcal{T}_0 \\ |1\rangle_A|0\rangle_B &\longrightarrow |0\rangle_A|1\rangle_B\mathcal{T}_1 + |0\rangle_A|1\rangle_B\mathcal{T}_a \end{aligned} \tag{8.40}$$

というコンパクトな形に表現できるので[8]，これにより光子通信路を定義する [394]．

光共振器はファイバとともに，その準モードのスペクトルや緩和定数などを定義する共鳴構造を持った合成光学系を構成する．光子吸収のみが起こる特別な場合には，式 (8.40) の演算子は単純な形になる．光周波数については，真空が環境の状態の非常によい近似となるので，$\mathcal{T}_0 = 1, \mathcal{T}_1 = \alpha(\tau) \sim e^{-\kappa\tau}, \mathcal{T}_a = \sum_j \beta_j(\tau) b_j^\dagger$，と書くことができる．ここで，$\sum_j |\beta_j(\tau)|^2 \sim 1 - e^{-2\kappa\tau}$ として，

[8] この種の表現では，左辺と右辺は両方とも，ある与えられた環境の状態へ作用するものと理解する．このコンパクトな表記法を用いると，通信路を 2 重かもしくはもっと複雑に作用させた場合において，表現をよりわかりやすいものにすることができる．

κ は（原子–）共振器–ファイバの全系の減衰率を，τ は転送時間を表す．演算子 $b_j^\dagger, b_j$ は，環境の j 番めの振動モードの振幅演算子である．

より一般的には，式 (8.40) の演算子 $\mathcal{T}_{0,1,a}$ は，原子の他の内部状態への遷移や，そこからのリポンピングだけではなく，自然放出や光子吸収も記述することができる．したがって，あらゆる複雑な物理が三つの演算子に隠されていることになる．この一般的な（非定常的な）状況では，環境を表す項の時間依存性を考慮に入れなくてはならない．演算子 $\mathcal{T}_{0,1,a}$ は転送が始まる初期時間に依存する．結果的に，通信路 (8.40) を繰り返し用いるときは，演算子の時間的な順序が重要になり，たとえば $\mathcal{T}_1(t_1)\mathcal{T}_0(t_0) \neq \mathcal{T}_0(t_1)\mathcal{T}_1(t_0)$ となる．

式 (8.38) のように EPR ペアを生成するために式 (8.40) を用いるときには，

$$[\alpha|0\rangle_A + \beta|1\rangle_A]\,|0\rangle_B \longrightarrow [\alpha|0\rangle_A|0\rangle_B\mathcal{T}_0 + \beta|1\rangle_A|1\rangle_B\mathcal{T}_1] + \beta|1\rangle_A|0\rangle_B\mathcal{T}_a \tag{8.41}$$

となる．$\alpha = \beta$ ならば，この表現は

$$|\Phi_{AB}^+\rangle\,[\mathcal{T}_0 + \mathcal{T}_1] + |\Phi_{AB}^-\rangle\,[\mathcal{T}_0 - \mathcal{T}_1] + \big(|\Psi_{AB}^+\rangle + |\Psi_{AB}^-\rangle\big)\,\mathcal{T}_a \tag{8.42}$$

という形に書ける[9]．ここで，ベル状態

$$|\Phi_{AB}^\pm\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B), \quad |\Psi_{AB}^\pm\rangle = \frac{1}{\sqrt{2}}\,(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$$

を用いた．結果として得られるペア (8.42) の忠実度は，理想的な結果 $|\Phi_{AB}^+\rangle$ との重なりで定義できる．この重なりはノルム

$$F = \left\| \frac{[\mathcal{T}_0 + \mathcal{T}_1]\,|E\rangle}{2} \right\|^2 \sim \left| \frac{1 + e^{-\kappa\tau}}{2} \right|^2 \tag{8.43}$$

で与えられる．2 番めの項において F を評価することによって，共振器–ファイバ系のモードと環境の相互作用が，EPR ペアの達成可能な忠実度をどのように減少させるのかがわかる．特に，F は，ファイバの対応する長さや転送時間とともに，指数関数的に減少する．

光子通信路の吸収長と同じかそれ以上の距離の間に EPR ペアを生成するためには，転送過程で起こり得る光子の損失を見つけ出して訂正する方法を

[9]この節では，必要とならない限り，規格化定数は省略する．

発見する必要がある．大雑把にいうと，(8.42) の吸収項 $\mathcal{T}_a$ をなくして，他の項 $\mathcal{T}_0 - \mathcal{T}_1$ を最小化しようとしている．

以下では，各共振器において一つか二つの補助原子を用いる方法の要点を述べる．この要約は本質的な手順をまとめているだけでなので，詳細は参考文献 [393]-[395] を参照のこと．

8.6.4 有限の手続きによる精製

情報を送信する前に，一つめの共振器内の原子を（予備の）補助原子とエンタングルさせるというのが，主なアイディアとなる．これは冗長符号化の方法を連想させるが，この方法は光子吸収の確率の**すべてのオーダ**のエラーを訂正できる点が基本的な違いである．受信者の共振器内にある二つの原子のある複合状態を測定することにより，送信された原子状態のはじめのコヒーレンスを**保ちながら**，光子損失を**検出する**ことができる．したがって，エラーがまったく検出されなくなるまで，送信を必要なだけ繰り返すことができる．

詳しく説明すると，次の三つの段階が必要となる．

(1) 原子状態を 3 粒子のエンタングルした状態へ**符号化する**．

$$\alpha|0\rangle_A + \beta|1\rangle_A \longrightarrow \alpha\left[|0\rangle_A|0\rangle_{A_2}|0\rangle_{A_3} + |1\rangle_A|1\rangle_{A_2}|1\rangle_{A_3}\right] + \beta\left[|0\rangle_A|0\rangle_{A_2}|1\rangle_{A_3} + |1\rangle_A|1\rangle_{A_2}|0\rangle_{A_3}\right] \qquad (8.44)$$

これは，A_3 と A の間，および A と A_2 の間にそれぞれ CNOT 操作を行うことにより実現される．

(2) 原子 A_2 と B_2 の間，それから A_2 と B の間において，式 (8.40) を用いて光子の**送信を 2 回行う**．その途中で A に局所的な反転操作を行う．この操作の結果，ここでは具体的な形は与えないが，多粒子のエンタングルした状態 [395] ができ上がる．

(3) 両方の共振器内にある予備の原子の状態を**測定する**．適当な局所的ユニタリ変換と合わせることにより，二つの結果のうちの一つを得る．

この過程の結果は，以下のような**吸収のない**（すなわち，訂正）通信路としてまとめられる．

$$\begin{array}{l} \big[\alpha|0\rangle_A+\beta|1\rangle_A\big]|0\rangle_B \longrightarrow \alpha|0\rangle_A|0\rangle_B\mathcal{S}_0+\beta|1\rangle_A|1\rangle_B\mathcal{S}_1 \\ \qquad\qquad \text{エラー}\searrow \quad \big[\alpha|0\rangle_A+\beta|1\rangle_A\big]|0\rangle_B\mathcal{S}_a \end{array} \tag{8.45}$$

2重の送信過程によって，式(8.45)の演算子$\mathcal{S}$は$\mathcal{T}$演算子の積となり，たとえば，$\mathcal{S}_0=\mathcal{T}_0\mathcal{T}_1, \mathcal{S}_1=\mathcal{T}_1\mathcal{T}_0$，または異なった順序のものになる．ステップ(3)での測定の結果に依存して，二つの結果があり得るということに注意することが重要である．もしエラーが検出されたら，状態は式(8.45)の2行めへ射影されて，送信を繰り返すことができる．もしエラーが検出されなければ，状態は式(8.45)の1行めへ射影されて，通信路を完了する．

式(8.40)の代わりに式(8.45)を用いると

$$\begin{aligned} [|0\rangle_A+|1\rangle_A]|0\rangle_B &\rightarrow |0\rangle_A|0\rangle_B\mathcal{S}_0+|1\rangle_A|1\rangle_B\mathcal{S}_1 \\ &= |\Phi^+_{AB}\rangle\frac{1}{2}[\mathcal{S}_0+\mathcal{S}_1]+|\Phi^-_{AB}\rangle\frac{1}{2}[\mathcal{S}_0-\mathcal{S}_1] \end{aligned} \tag{8.46}$$

が得られる．

式(8.40)の後で考えた単純な例では，$\mathcal{T}=1$および$\mathcal{T}_1=e^{-\kappa\tau}$とすることにより，$\mathcal{S}_0=e^{-\kappa\tau}$と$\mathcal{S}_1=e^{-\kappa\tau}$を得るので，式(8.46)の第2項は消える．この状況では，通信路(8.45)を**1回**使えば理想的なEPRペアができ上がる．このことは，光子送信の平均数が$e^{2\kappa\tau}$であることに対応する．

より一般的には，環境の状態が演算子$\mathcal{T}_0$と$\mathcal{T}_1$の時間的な順序に依存しないときに，似たような結果が得られる．そのような**定常的な環境**は$\mathcal{T}_1(t_1)\mathcal{T}_0(t_0)|E\rangle=\mathcal{T}_0(t_1)\mathcal{T}_1(t_0)|E\rangle$，すなわち，$\mathcal{S}_0|E\rangle=\mathcal{S}_1|E\rangle$によって定義される．定常的な環境のもとにある任意の系では，式(8.45)を1回適用すれば理想的なEPRペアが生成される．

一般の非定常的な場合の議論のために，まずはじめに式(8.46)の結果を次のように書き直そう．

$$|\Psi^{(1)}\rangle=|\Phi^+_{AB}\rangle|E^{(1)}_+\rangle+|\Phi^-_{AB}\rangle|E^{(1)}_-\rangle \tag{8.47}$$

ここで，$|E^{(1)}_\pm\rangle=\frac{1}{2}(\mathcal{S}_0\pm\mathcal{S}_1)|E\rangle$である．環境$|E^{(1)}_+\rangle$のノルム（の2乗）によってペアの忠実度が決まる．

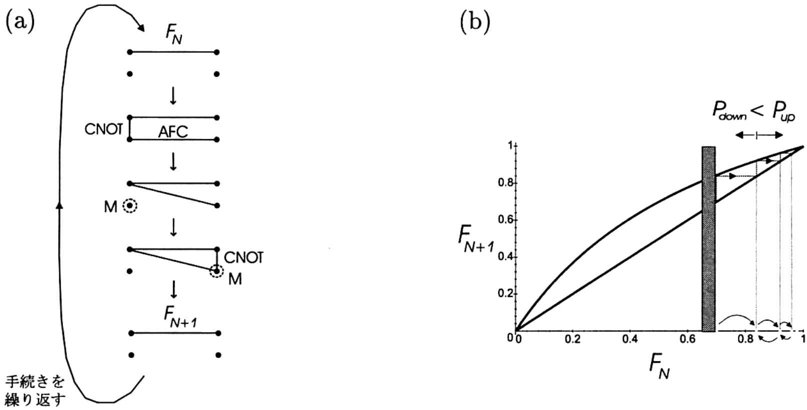


図 8.13 有限の手続きによる EPR ペアの精製.
(a) 繰り返し精製プロトコル．各精製段階において，式 (8.48) の形をした忠実度 F_N の EPR ペアは，二つの補助原子と一時的にエンタングルしている．これは二つの CNOT 演算と吸収のない通信路 AFC，測定 M から構成される．さらに，図には示されていないアダマール変換がいくつかある．新しい忠実度 F_{N+1} の値は，(b) に説明があるように，測定 M の結果に依存する．この方法は，各段階において原子の同じ集合に対して作用するので「自己精製過程」をなすことに注意せよ．
(b) 忠実度の片側だけへのランダムウォーク過程．(a) での各繰り返し過程の後，忠実度 F_N は N に依存するある確率 $P_{\mathrm{up}}(P_{\mathrm{down}})$ とともに増加（減少）する．もし F_N が初期値 F_0 より下に落ちてしまったら，式 (8.46) にあるように AFC を 1 回使って，ペアをこの値まで引き戻す．これは，図に示されているように，F_0 という境界での反射による片側だけへのランダムウォーク過程に等価である．平均すると忠実度は指数関数的に 1 に近づく，$F_N \sim 1 - e^{-\mathrm{const.}} \times N$

ここで，吸収のない通信路 (AFC) の重要な利点が効いてくる．すなわち，コヒーレンスと，それが適用される状態のエンタングルメントを保ちながらも，伝送過程におけるエラーが訂正されるのである．これによって，繰り返しの精製プロトコルが可能になる [394]．各精製段階において，局所的な CNOT 演算と AFC を用いることにより，各ノードにある二つの補助原子とそのペアは一時的にエンタングルする．ある意味では，式 (8.47) を精製するために使われる補助的な EPR ペアが，これによって生成されることになる．プロトコルの詳細は図 8.13(a) に体系的に示してある．

このプロトコルは，式 (8.47) を次の形の状態の列に変換する．

$$|\Psi^{(N)}\rangle = |\Phi^+_{AB}\rangle|E^{(N)}_+\rangle + |\Phi^-_{AB}\rangle|E^{(N)}_-\rangle \tag{8.48}$$

ここで，測定結果に応じて

$$|E^{(N)}_\pm\rangle = \frac{1}{2}(\mathcal{S}_0 \pm \mathcal{S}_1)|E^{(N-1)}_\pm\rangle, \quad \text{または} \quad |E^{(N)}_\pm\rangle = \frac{1}{2}(\mathcal{S}_0 \mp \mathcal{S}_1)|E^{(N-1)}_\pm\rangle$$

となる．1 番めの場合は確率 $P_{up} = P^{(N)}_{up}$ で起きるのだが，ペアの忠実度は増加する．2 番めの場合は確率 $P_{down} = 1 - P^{(N)}_{up}$ で起きるのだが，ペアの忠実度は減少する．これによって，図 8.13(b) に示すような，片側だけへのランダムウォークに対応する確率過程が形成されることを示すことができる．平均すると，忠実度 $F_N = \langle E^{(N)}_+|E^{(N)}_+\rangle$ は精製過程の回数とともに，指数関数的に 1 に収束する．

8.7　量子中継器

前の節で議論した方法を用いると，原子をつないでいる，散逸と雑音のある通信路を通して光子を送ることにより，忠実度の高い EPR ペアを作ることができる．しかし，通信路での伝送時間が緩和時間よりもだいぶ長くなってしまうと，つまり，もし $\kappa\tau \gg 1$ であると，この方法には限界がある．吸収確率が τ とともに指数関数的に増加するにつれて，伝送を成功させるのに必要な繰り返し回数も同様に増加することになる．

吸収損失は古典通信路を通した電気信号の伝送の問題においてよく知られていて，通信路上に，規則正しい間隔で中継器が置かれている．古典的な（デジタル）通信技術においては，そのような中継器は信号を増幅して復元するために使われる．中継器の間の距離は，ファイバの減衰率と伝送のビット率によって決まる（分散効果）．

量子通信では増幅器を使うことができない．EPR 相関を作るためには量子ビット（光子）を伝送する必要があるが，量子相関を壊さずにそれらを増幅させることはできない [88,396]．ここでできることは，光子が吸収されたかどうかを検知して，もしそうなら，そのときは伝送を繰り返すことだけである．

以下の議論では，主要な伝送エラーは光子吸収によるものであり，環境は定常的だと仮定しよう．このことは，光子通信路 (8.40) において $\mathcal{T}_0 = 1$，お

よび $\mathcal{T}_1 = e^{-\kappa\tau} = e^{-l/2l_0}$ としたものに対応する．ここで，$l_0 = c/2\kappa$ は以下においてファイバの半値長と呼ぶ量を定義するものとする．量子ビットの A から B への伝送に成功する確率は，図 8.14（上）に示すように，l をファイバの長さとして $p(l) = e^{-l/l_0}$ となる．それに対応して，必要な繰り返し回数の平均は

$$n(l) = \frac{1}{p(l)} = e^{l/l_0} \tag{8.49}$$

となる．もしファイバが半値長 l_0 よりもかなり長ければ，どんな実験でも非現実的に多くの回数が必要になるのはこのことから明らかである．

古典通信における中継器の考え方に従って，通信路を N 個の区間に分割して，その各区間の間に伝送エラーが起きたかどうかを観測する接続点（ノード）を置く（図 8.14（下）参照）．これは，たとえば 5.2 節で解説した方法で，共振器内の二，三の余分なイオンを用いることにより可能となる．もし吸収エラーが検出されたら，その区間での伝送を繰り返す．それから，光子は引き続く区間に送信されるなどとなる．したがって，理想的には，A にある原子の状態は原子 B にたどり着くまで，ある接続点から次の接続点へと交換されていく．各区間での全繰り返し回数の平均は，$n(l/N) = e^{l/l_0 N}$ となる．それに対応して，**合成ファイバ**を通して量子ビットの送信を成功させるのに必要な伝送回数は

$$n_{\text{com}} = \frac{N}{p(l/N)} = Ne^{l/Nl_0} \tag{8.50}$$

となる．これを式 (8.49) と比べてみるべきであり，もし，

$$Ne^{l/Nl_0} < e^{l/l_0} \tag{8.51}$$

であれば，単純なファイバより合成ファイバのほうがよいという結果になる．最適な区間の数は，上記の式の左辺を最小化する N の値によって与えられる．つまり，$N_{\min} = l/l_0$ となる．合成ファイバでの伝送回数の最小値は式 (8.50) において $N = N_{\min}$ とすることによって得られる．

$$n_{\min} = N_{\min} e^{l/N_{\min} l_0} = l/l_0 e^1 \tag{8.52}$$

接続点が半値長 l_0 に対応する間隔をあけて設置されていれば，この状況は実現される．

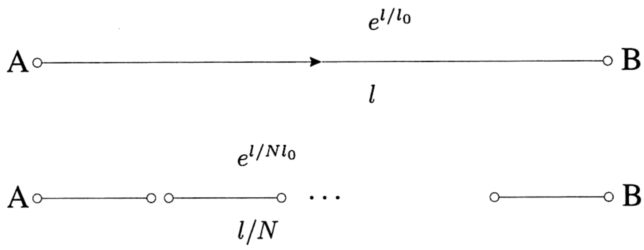


図 8.14　単純なファイバと合成ファイバを用いた A から B への量子ビットの伝送．古典的な中継器のように，一つの量子ビットを長い距離伝送するには，ファイバ（通信路）をいくつかの区間に分割して，各区間の終点で伝送エラーを観測する

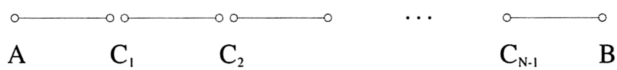


図 8.15　N 個の EPR ペアの列の接続．本文を参照

ここまでは，局所的操作がエラーなしで行えると仮定してきた．実際，局所的な 2 ビット操作におけるエラーを検知して訂正する方法 [397] が存在する．しかし，たとえこの方法を用いても，検出機構そのものが用いる 1 ビットの操作と測定が不完全かもしれないので，エラーが検出を免れる可能性がある．これにより二つのことが引き起こされる．(i) 図 8.14（下）の各チェックポイントでの局所的操作により，伝送過程に雑音が入る．(ii) 各区間における伝送の忠実度は，ある最大値 $F_{\max}$ にすでに制限されている．吸収のない通信路 (8.45) と図 8.13(a) の精製プロトコルがともに，雑音を引き起こして最大忠実度を制限するような局所的操作を含むという事実から，このことがわかる．両方の効果がチェックポイントの数とともに（指数関数的に）蓄積して，結局は伝送の忠実度を完全にだめにしてしまう．

この点をはっきりさせるために，以下のような等価な問題を考えてみよう．はじめに，図 8.15 にあるように，忠実度が $F_1 < F_{\max}$ である N 個の単純な EPR ペアを，ノード A と C_1，C_1 と C_2，…，C_{N-1} と B の間に作る．それから，テレポーテーション [74] やエンタングルメント・スワッピング [74,398] のように，各ノード C_i においてベル測定を行い，その結果をノード間で古典通信を用いて伝え合うことによりこれらのペアを接続する．これによって，

図 8.15 のように，両端の A と B の間に一つの EPR ペアができ上がる．残念ながら，雑音を引き起こすような不完全な操作を接続過程が含むので，結果としてでき上がるペアの忠実度は接続のたびに減少する．さらに，完璧な接続をしても忠実度は下がってしまう．たとえば，忠実度が F_1 であるような二つの Werner 状態を，ベル測定を用いて接続すると

$$F_2 = \frac{1}{4}\left\{1 + 3\left(\frac{4F-1}{3}\right)^2\right\} \tag{8.53}$$

という忠実度の新しい Werner 状態を得るので，$F_2 \sim F_1^2$ となるのは，$F_1 \sim 1$ のときである．両方の効果が各接続ごとに蓄積して，A と B の間の最終的なペアの忠実度 F_N が，N とともに指数関数的に減少してしまうことになる．結局，F_N の値は，それ以下に落ちるともう精製できなくなってしまうようなある限界値 $F_{\min} \geq 1/2$ より下に落ちてしまう．このことは，精製によって忠実度を上げることはできないことを意味する [47,49].

通信路をより短い区間に分割することにより，必要な伝送回数が指数関数的に増加してしまうという効果をなくすことができたように見えるが，忠実度が指数関数的に減少してしまうという犠牲を払うことになってしまった！

この制限を避ける方法としては，$F_L > F_{\min}$ となって精製が可能となるように，より少ない数の $L \ll N$ 個のペアを接続することが考えられる．結果として生じるペアを接続して，再び精製して，ということを，同様に続けるというのがアイディアである．このように接続と精製を交互に行う方法は，N つまり l とともに，必要な資源の数が指数関数的に増加しないように，うまく設計されていなくてはならない．

この節の残りの部分では，以下の意味において，ペアの接続と精製を同時に行う**入れ子状の精製プロトコル** [381] を解説する（図 8.16 を参照）．単純化するために，ある整数 n に対して，$N = L^n$ と仮定する．第 1 段階では,（初期忠実度が F_1 である）ペアを $C_L, C_{2L}, \ldots, C_{N-L}$ 以外のすべての接続点で同時に接続する．結果として，A と C_L，C_L と C_{2L} の間などに（忠実度が F_L で）長さが L のペアが N/L 個でき上がる．これらのペアを精製するために，同様の方法で作られた M 個のコピーが必要である．この方法がどのように進んでいくのかを見るには，図 8.16 に示した $L = 3, M = 4$ の場合のように，基本的なペアを配列すると便利である．それから，区間 A と C_L，C_L と C_{2L}

などにあるそれらのコピーを用いて，各区間において忠実度 F_1 のペアを精製して（再び）得る．この最後の条件によって，必要なコピーの（平均）数 M が決まるのだが，その数は初期忠実度と，接続時における忠実度の劣化，精製プロトコルの精度によって決定される．この時点までに使った基本的なペアの総数は LM となる．[図 8.16 において，このことは，$L \times M = 3 \times 4$ 個のペアを含む各グループがはじめの忠実度をもった一つのペアに置き換えられたことを意味する．] 第 2 段階では，$C_{L^2}, C_{2L^2}, \ldots, C_{N-L^2}$ 以外のすべての接続点 $C_{kL}(k = 1, 2, \cdots)$ において，これら L 個の大きなペアを接続する．結果として，A と C_{L^2}，C_{L^2} と C_{2L^2} の間などに，忠実度が F_L で長さが L^2 のペアが N/L^2 個でき上がる．再び，F_1 以上の忠実度に再精製するために，これらの長いペアも M 個のコピーが必要になる．この時点までに必要になった基本的なペアの総数は $(LM)^2$ である．[これで，図 8.16 の $3^2 \times 4^2$ 個のペアの配列全体は忠実度 F_1 の一つのペアで置き換えられたことになる．] この過程を，段階を次々と上げて，第 n 段階まで繰り返す．その結果，A と B の間に忠実度が F_1 で長さが L の最終的なペアができ上がる．このようにして，基本的なペアの総数 R は $(LM)^n$ となる．ここで，M^n 単独では図 8.16 の必要な「平行な通信路」の数を表す．この結果を

$$R = N^{\log_L M + 1} \tag{8.54}$$

という形にあらためて表現することができて，これは必要な資源が距離 N とともに**多項式的に**増加することを表す．

入れ子状の精製プロトコルの考え方は，フォールトトレラント量子計算 [400] で使われる連接符号化 [399] の考え方と関係がある．その方法を用いると，原理的には，多項式程度の資源しか使わずに任意の長い距離の量子ビットの伝送が可能になる．しかし，一つの量子ビットを，たくさんの量子ビットからなるエンタングルした状態に符号化してから通信路で送り，さらに，伝送過程の間はこの符号を繰り返し操作する必要がある．対照的に，入れ子状の精製の方法では，任意の量子ビットを通信路を通して送信するのではなく，全通信路にわたって，EPR 相関を同時に作るのである．相関を作り上げる間は，実際には量子情報は何も処理されない（その EPR ペアはその後にテレポーテーションによる通信で使われるかもしれないが）．その結果，局所的操作の忠実度に対する要求は数パーセント程度となる．フォールトトレラント量

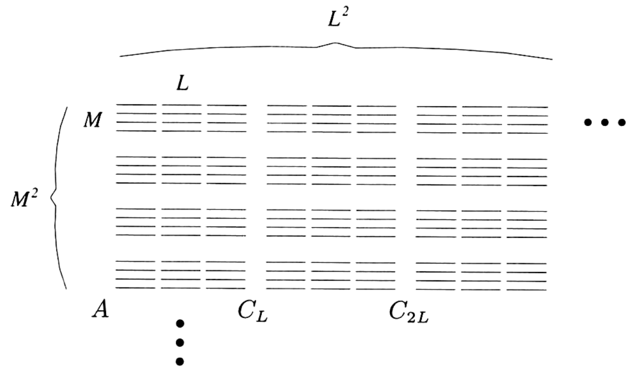


図 8.16 基本的な EPR ペアの配列に対する入れ子状の精製

子計算の場合は，この数は 10^{-5} のオーダーとなる [399].

図 8.16 の配列は，精製を行う同一の（基本的な）EPR ペアのアンサンブルを表す．代わりに，各段階において一つの補助的なペアの助けを借りて精製を行うこともできる（[381],[387] 参照）．ある意味では，図 8.16 の図式における垂直方向の次元は，時間的な軸（繰り返しの回数）と解釈できる．この場合，式 (8.54) のように多項式的に増加するのは，A と B の間に EPR ペアを作り上げるのに必要な全**時間**だが，各接続部分で必要な予備の原子の数は，$N = l/l_0$ とともに対数関数的に増加するだけである．量子中継器の最終的な方法は，図式的には図 8.17 のようになる．通信路上の各接続点は，精製に必要なゲート操作や測定を施す少数の原子を含んだ単純な「量子プロセッサ」からなる．たとえば，8.6 節で解説した方法を用いて，隣り合う接続点（ここでは，$L = 2$）の間に EPR ペアを繰り返し作るために使われる原子もある．繰り返し生成されたこれらのペアは，エンタングルメント精製に用いられる．より遠く離れたペアは，エンタングルメント・スワッピングによって生成される．これらの，より離れたペアを（再）精製するために，各段階で一つの補助的な原子を蓄えておく必要がある．したがって，各プロセッサが保持しなくてはならない総数は，l とともに単に対数関数的に増加する [381,387].

古典通信の場合とは対照的に，量子中継器は局所的な増幅器ではないが，局所的なチェックポイントと大局的な（入れ子状の）精製プロトコルの両方を含んでいる．ここでは，われわれの方法が局所的操作と測定に対して数パー

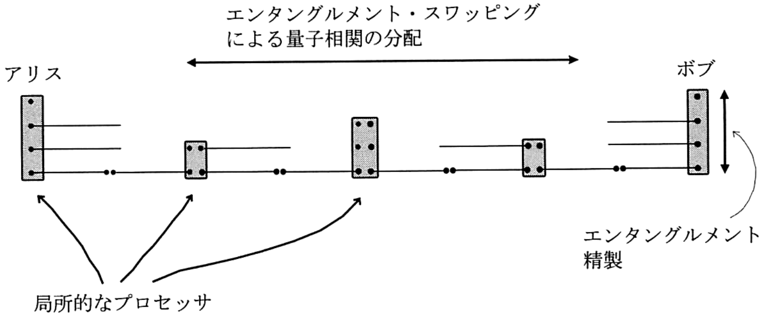


図 8.17　量子中継器の方法．各接続点では，エンタングルメント精製とエンタングルメント・スワッピングのプロトコルを実行するために（二，三の量子ビットだけからなる）小さな「量子プロセッサ」を用いる．合成通信路を用いた高い忠実度のエンタングルメントの分配は，入れ子状のエンタングルメント精製 [381] と呼ばれる大局的なプロトコルによって組織される

セントの範囲でエラーに強いことを報告しただけなので，より詳しくは参考文献 [381,387] を参照のこと．

参考文献

1. R.P. Feynman, R.B. Leighton, and M. Sands, *The Feynman Lectures of Physics, Vol. III, Quantum Mechanics*, Addison-Wesley, Reading (1965).
2. G.I. Taylor, Proc. Camb. Phil. Soc. **15**, 114 (1909).
3. G. Möllenstedt and C. Jönsson, Z. Phys. **155**, 472 (1959); A. Tonomura, J. Endo, T. Matsuda, and T. Kawasaki, Am. J. Phys. **57**, 117 (1989).
4. A. Zeilinger, R. Gähler, C.G. Shull, W. Treimer, and W. Mampe, Rev. Mod. Phys. **60**, 1067 (1988).
5. O. Carnal and J. Mlynek, Phys. Rev. Lett. **66**, 2689 (1991).
6. S.L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).
7. A. Zeilinger, Am. J. Phys. **49**, 882 (1981).
8. M.P. Silverman, *More than One Mystery: Explorations in Quantum Interference*, Springer, Berlin (1995).
9. E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik", Naturwissenschaften, **23**, 807; 823; 844 (1935). English translation, "The Present Situation in Quantum Mechanics", Proc. of the American Philosophical Society, **124**, 323 (1980); reprinted in *Quantum Theory and Measurement* edited by J.A. Wheeler and W.H. Zurek, Princeton, 152 (1983).
10. M.A. Horne and A. Zeilinger, in: *Proceedings of the Symposium Foundations of Modern Physics*, P. Lahti, P. Mittelstaedt (Eds.), World Scientific, Singapore 435 (1985); M.A. Horne and A. Zeilinger, in: *Microphysical Reality and Quantum Formalism*, A. van der Merwe, et al. (Eds.), Kluwer, Dordrecht, 401 (1988).
11. J.S. Bell, Phys. World **3**, 33 (1990).

12. J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
13. D. Greenberger, M.A. Horne, A. Zeilinger, *Going beyond Bell's Theorem, in "Bell's Theorem, Quantum Theory, and Conceptions of the Universe"*, M. Kafatos (Ed.), Kluwer, Dordrecht, 69 (1989).
14. N.D. Mermin, Phys. Today **43**, No. 6, 9 (1990); D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
15. D. Bohm, *Quantum Theory*, Prentice-Hall, Englewood Cliffs, 614 (1951).
16. P.G. Kwiat, H. Weinfurter, T. Herzog, and A. Zeilinger, Phys. Rev. Lett. **74**, 4763 (1995).
17. K.F. Weizsäcker, Z. Phys. **40**, 114 (1931).
18. D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
19. D. Bruss, A. Ekert, F. Huelga, J.-W. Pan, and A. Zeilinger, Phil. Trans. R. Soc. (London) A **355**, 2259 (1997).
20. N. Bohr, "Discussions with Einstein on Epistemological Problems in Atomic Physics" in *Albert Einstein: Philosopher-Scientist*, Edited by P.A. Schilpp, The Library of Living Philosophers, Evanston, 200 (1949).
21. A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
22. N. Bohr, Phys. Rev. **48**, 696 (1935).
23. J.S. Bell, *On the Einstein-Podolsky-Rosen paradox*, Physics **1**, 195 (1964), reprinted in J.S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge U.P., Cambridge (1987).
24. S.J. Freedman and J.S. Clauser, Phys. Rev. Lett. **28**, 938 (1972); A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **47**, 1804 (1982); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998); G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
25. A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); **49**, 91 (1982); A. Aspect, J. Dalibard, and G. Roger, ibid. **49**, 1804 (1982).
26. P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y.H. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
27. P.M. Pearle, Phys. Rev. D **2**, 1418 (1970); J.F. Clauser, A. Shimony, Rep. Prog. Phys. **41**, 1881 (1978).
28. E.P. Wigner, Am. J. Phys. 38, 1005 (1970).
29. D. Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan, New York (1967).
30. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1996).

31. B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, John Wiley & Sons (1994).
32. D. Welsh, *Codes and Cryptography*, Clarendon Press, Oxford, (1988).
33. C.E. Shannon, Bell Syst. Tech. J, **28**, 656 (1949).
34. W. Diffie, and M.E. Hellman, IEEE Trans. Inf. Theory, **IT-22**, 644 (1976).
35. R. Rivest, A. Shamir, and L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
36. P. Shor, (1994) *Proc. of 35th Annual Symposium on the Foundations of Computer Science*, (IEEE Computer Society, Los Alamitos), p. 124 (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing, **26** (1997), 1484 and is also available at quant-ph/9508027.
37. S. Wiesner, *SIGACT News*, **15**, 78 (1983); original manuscript written *circa* 1970.
38. C.H. Bennett and G. Brassard, in *"Proc. IEEE Int. Conference on Computers, Systems and Signal Processing"*, IEEE, New York, (1984).
39. J.F. Clauser and M.A. Horne, *Phys. Rev. D* **10**, 526 (1974).
40. B. Huttner and A. Ekert, J. Mod. Opt., **41**, 2455 (1994).
41. P.D. Townsend, Nature **385**, 47 (1997).
42. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
43. A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
44. A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69** 1293 (1992).
45. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
46. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
47. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996); C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
48. Q.A. Turchette, C.J. Hood, W. Lange,H. Mabuchi, and H.J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).
49. Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A., Wootters, W. K. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys. Rev. Lett. **76**, 722-725 (1996).
50. M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78** 574 (1997).
51. G. Brassard and L. Salvail, *Eurocrypt '93, Lofthus, Norway* (1993).
52. B.A. Slutsky, R. Rao, P.-C. Sun and Y. Fainman, Phys.Rev.A **57**, 2383 (1998).

53. J.I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
54. C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
55. H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
56. N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
57. C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, *1994 IEEE International Symposium on Information Theory*, Trondheim, Norway, June (1994).
58. A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, (1995).
59. E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, *Security of Quantum Key Distribution against all Collective attacks*, quant-ph/9801022 (1998).
60. D. Mayers, *Unconditional security in Quantum Cryptography*, quant-ph/9802025 (1998).
61. M.N. Wegman, J.L. Carter, Journal of Computer and System Sciences **22**, 265-279 (1981).
62. G. Ribordy, J.D. Gautier, H. Zbinden, and N. Gisin, Applied Optics **37**, 2272 (1998).
63. R.Y. Chiao and Y.S. Wu, Phys. Rev. Lett. **57**, 933 (1986).
64. B.C. Jacobs and J.D. Franson, Opt. Lett. **21**, 1854 (1996).
65. W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, Los Alamos preprint, quant-ph/9805071.
66. P.D. Townsend, C. Marand, S.J.D. Phoenix, K.J. Blow, and S.M. Barnett, Phil. Trans. Roy. Soc. London A **354**, 805 (1996).
67. R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, C.G. and C. Simmons, C. *Quantum cryptography over underground optical fibres*, Advances in Cryptology - Proceedings of Crypto'96, Springer, Berlin, Heidelberg (1996).
68. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electronics Letters **34**, 2116-2117 (1998).
69. J.D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).
70. J.G. Rarity, P.C.M. Owens, and P.R. Tapster, Phys. Rev. Lett. **73**, 1923 (1994).
71. W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden and N. Gisin, Phys. Rev. A **57**, 3229 (1998); W. Tittel, J. Brendel, H. Zbinden and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
72. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys.

Rev. Lett. **81**, 5039 (1998).

73. C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett., **69**, 2881 (1992).
74. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
75. K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).
76. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation. Nature **390**, 575-579 (1997).
77. S. Popescu, LANL E-print quant-ph 9501020.
78. D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).
79. L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
80. S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
81. A. Furusawa, J.Ł. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Science Oct23 1998 pp 706-709.
82. Comment by F. De Martini, and Reply by A. Zeilinger, Physics World **11**, nr.3, 23-24 (March 1998).
83. Comment by S.L. Braunstein and H.J. Kimble, and Reply by D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, M. Zukowski, and A. Zeilinger, Nature (London) **394**, 840-841 (1998).
84. D. Bouwmeester, J.-W. Pan, H. Weinfurter, and A. Zeilinger, High-fidelity teleportation of qubits, J. Mod. Opt. **47**, 279 (2000).
85. M. Zukowski, A. Zeilinger, M.A. Horne, and A. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
86. J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental entanglement swapping: Entangling photons that never interacted. Phys. Rev. Lett. **80**, 3891-3894 (1998).
87. S. Bose, V. Vedral, and P.L. Knight, *A multiparticle generalisation of entanglement swapping* Phys. Rev. A **57**, 822 (1998).
88. W.K. Wootters and W.H. Zurek, Nature (London) **299**, 802, (1982).
89. D.N. Klyshko, Sov. Phys. JETP **28**, 522 (1969).
90. D.C. Burnham and D.L. Weinberg, Phys. Rev. Lett. **25**, 84 (1970).
91. J.D. Franson and K.A. Potocki, Phys. Rev. A **37**, 2511 (1988).
92. J. Brendel, E. Mohler, and W. Martiennsen, Europhys. Lett. **20**, 575 (1992); P.G. Kwiat, A.M. Steinberg and R.Y. Chiao, Phys. Rev. A **47**, R2472 (1993).
93. J. Brendel, N. Gisin, W. Tittel and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).

94. J.G. Rarity and P.R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990).
95. R. Loudon, *Coherence and Quantum Optics VI*, ed. Eberly, J.H. and Mandel, L. Plenum New York, 703 (1990).
96. A. Zeilinger, H.J. Bernstein, and M.A. Horne, J. Mod. Optics, **41**, 2375, (1994).
97. H. Weinfurter, Europhys. Lett. **25**, 559 (1994).
98. S.L. Braunstein and A. Mann, Phys. Rev. **A 51**, R1727 (1995).
99. M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).
100. A. Zeilinger, *Proc. of the Nobel Symp. 104* "Modern Studies of Basic Quantum Concepts and Phenomena" E.B. Karlsson and E. Brändes (Eds.), Physica Scripta, T76, 203 (1998).
101. M. Zukowski, A. Zeilinger and H. Weinfurter in *Fundamental Problems in Quantum Theory* vol. 755 Annals of the New York Academy of Sciences (Greenberger and Zeilinger Eds.) p. 91 (1995).
102. J. Kim, S. Takeuchi, Y. Yamamoto, and H.H. Hogue, Appl. Phys. Lett, **74**,902 (1999).
103. E. Hagley, X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond, and S. Haroche, Generation of Einstein-Podolsky-Rosen pairs of atoms. Phys. Rev. Lett. **79**, 1-5 (1997).
104. H-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
105. M. Zukowski, Phys. Lett. A 157, 198 (1991).
106. R. Loudon, *The Quantum Theory of Light, second edition.* Clarendon Press, Oxford, (1983).
107. A. Yariv, *Quantum Electronics, third edition.* John Wiley& Sons (1989).
108. D.F. Walls and G.J. Milburn, *Quantum Optics, second edition.* Springer, Berlin, Heidelberg (1994).
109. P.W. Milonni, *The Quantum Vacuum* Academic Press, San Diego, 1994.
110. Z.Y. Ou, S.F. Pereira, H.J. Kimble, and K.C. Peng, Rhys. Rev. Lett. **68**, 3663 (1992).
111. Z.Y. Ou, S.F. Pereira, and H.J. Kimble, Appl. Phys. B **55**, 265 (1992).
112. H.J. Kimble, in *Fundamental Systems in Quantum Optics, Les Houches, 1990*, eds. J. Dalibard, J.M. Raimond, J. Zinn-Justin (Elsevier Science Publishers, Amsterdam, 1992), pp, 549-674.
113. Ling-An Wu, H.J. Kimble, J.L. Hall, and Huifa Wu, Phys. Rev. Lett. **57**, 2520 (1986).
114. See, for example, S.J. Freedman and J.S. Clauser, Phys. Rev. Lett **28**, 938 (1972).

115. M. Lamehi-Rachti and W. Mittig, Phys. Rev. D **14**, 2543 (1976).
116. E. Biham, B. Huttner and T. Mor, Phys. Rev. A **54**, 2651 (1996).
117. C.H Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
118. S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **60**, 194 (1999).
119. A. Zeilinger, M.A. Horne, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett **78**, 3031 (1997).
120. L. Grover, *Proc. 28 Annual ACM Symposium on the Theory of Computing*, ACM Press New York, 212 (1996).
121. G. Brassard, Science **275**, 627 (1997).
122. R. Rivest, A. Shamir, and L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).
123. R. Feynman, Int. J. Theor. Phys. **21**, 467, (1982).
124. D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).
125. D. Deutsch, Proc. R. Soc. London A: **425**, 73, (1989).
126. S.F. Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M.B. Plenio, and J.I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).
127. D. Deutsch, *The Fabric of Reality* (Allen Lane, Penguin Press, London).
128. D. Deutsch and A. Ekert, Phys. World **11**, 47 (March 1998).
129. A. Barenco, C.H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
130. D. Deutsch, A. Barenco, and A. Ekert, Proc. Roy. Soc. Lond. A **449**, 669 (1995).
131. C.H. Papadimitriou, *Computational Complexity* (Addison-Wesley, Reading, MA, 1994).
132. M. Garey, and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP Completeness* (W. H. Freeman and Co., 1979).
133. R. Jozsa, Entanglement and Quantum Computation in *The Geometric Universe*, 369, eds. S. Huggett, L. Mason, K.P. Tod, S.T. Tsou and N.M.J. Woodhouse (Oxford University Press, 1998).
134. A. Ekert and R. Jozsa, Phil. Trans. Roy. Soc. London Ser A, **356**, 1769 (1998).
135. A.S. Holevo, Probl. Inf. Transm **9**, 177 (1973).
136. C. Fuchs and A. Peres, Phys. Rev. A. **53**, 2038 (1996).
137. T. Cover and J. Thomas, *Elements of Information Theory,* John Wiley and Sons (1991).
138. D. Deutsch and R. Jozsa, Proc. Roy. Soc. Lond. A **439**, 553 (1992).
139. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. Roy. Soc. Lon-

don Ser A, **454**, 339 (1998).

140. E. Bernstein and U. Vazirani, *Proc. 25th Annual ACM Symposium on the Theory of Computing*, (ACM Press, New York), p. 11-20 (1993) (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing, **26**, 1411 (1997).
141. D. Simon, (1994) *Proc. of 35th Annual Symposium on the Foundations of Computer Science*, (IEEE Computer Society, Los Alamitos), p. 116 (Extended Abstract). Full version of this paper appears in S. I. A. M. Journal on Computing, **26**, 1474 (1997).
142. G.H. Hardy and E.M. Wright *An Introduction to the Theory of Numbers* (4th edition, Clarendon, Oxford, 1965).
143. M.R. Schroeder, *Number Theory in Science and Communication* (2nd enlarged edition, Springer, New York, 1990).
144. A. Ekert and R, Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
145. D.K. Maslen and D.N. Rockmore, "Generalised FFT's – A Survey of Some Recent Results", in *Proc. DIMACS Workshop on Groups and Computation – II* (1995).
146. R. Jozsa, Proc. Roy. Soc. London Ser A, **454**, 323 (1998).
147. G. Brassard and P. Hoyer, "An exact polynomial-time algorithm for Simon's problem", *Proc. 5th Israeli Symposium on Theory of Computing and Systems (ISTCS 97)*, 12 (1997), also available at quant-ph/9704027.
148. A. Kitaev, Russian Math. Surveys **52**, 1191 (1997), also available at quant-ph/9511026.
149. R. Beals, *Proc. 29th Annual ACM Symposium on the Theory of Computing – STOC* (ACM Press, New York), 48 (1997).
150. L. Grover, Phys. Rev. Lett.**78**, 325 (1997).
151. M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, *Proc. of fourth workshop on Physics and Computation – PhysComp'96*, 36-43 (1996).
152. L. Grover, "A Framework for Fast Quantum Algorithms", *Proc. 30th ACM Symposium on Theory of Computation (STOC'98)*, 53 (1998), also available at quant-ph/9711043.
153. G. Brassard, P. Hoyer, and A. Tapp, "Quantum Counting", *Proc. 25th ICALP*, Vol 1443, Lecture Notes in Computer Science, 820 (Springer, 1998), also available at quant-ph/9805082.
154. L. Grover, Phys. Rev. Lett. **80**, 4325 (1997).
155. C.H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, S. I. A. M. Journal on Computing, **26**, 1510 (1997).
156. J.I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
157. J.F. Poyatos, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998).

158. C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).

159. E.T. Jaynes and F.W. Cummings, Proc. IEEE **51**, 89 (1963).

160. *Cavity Quantum Electrodynamics, Advances in atomic, molecular and optical physics, Supplement 2*, P. Berman editor, Academic Press (1994).

161. S. Haroche, in *Fundamental systems in quantum optics, les Houches summer school session LIII*, J. Dalibard, J.M. Raimond and J. Zinn-Justin eds, North Holland, Amsterdam (1992).

162. D.G. Hulet and D. Kleppner, Phys. Rev. Lett. **51**, 1430 (1983).

163. P. Nussenzvzeig, F. Bernardot, M. Brune, J. Hare, J.M. Raimond, S. Haroche and W. Gawlik, Phys. Rev. A **48**, 3991 (1993).

164. M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernardot, A. Maali, J.M. Raimond, and S. Haroche, Phys. Rev. Lett, **72**, 3339 (1994).

165. M. Brune, F. Schmidt-Kaler, A. Maali, J. Dreyer, E. Hagley, J.M. Raimond, and S. Haroche, Phys. Rev. Lett. **76**, 1800 (1996).

166. M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J.M. Raimond, and S. Haroche, Phys. Rev. Lett.,**77**, 4887 (1996).

167. X. Maître, E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. Lett. **79**, 769 (1997).

168. E. Hagley, X. Maître, G. Nogues, C. Wunderlich, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. Lett. **79**, 1 (1997).

169. G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J.M. Raimond and S. Haroche, Nature **400**, 239 (1999).

170. G. Raithel, C. Wagner, H. Walther, L.M. Narducci and M.O. Scully, in *Cavity Quantum Electrodynamics*, P. Berman ed. 57, Academic, New York (1994).

171. J.H. Eberly, N.B. Narozhny and J.J. Sanchez–Mondragon, Phys. Rev. Lett. **44**, 1323 (1980).

172. R.J. Thompson, G. Rempe and H.J. Kimble, Phys. Rev. Lett. **68**, 1132 (1992).

173. F. Bernardot, P. Nussenzveig, M. Brune, J.M. Raimond and S. Haroche, Euro. Phys. Lett. **17**, 33 (1992).

174. P. Domokos, J.M. Raimond, M. Brune and S. Haroche, Phys. Rev. A **52**, 3554 (1995).

175. J.I. Cirac and P. Zoller, Phys. Rev. A **50**, R2799 (1994).

176. D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am.J.Phys **58**, 1131 (1990). N.D. Mermin, Physics Today (June 9, 1990).

177. S. Haroche in *Fundamental problems in quantum theory*, D. Greenberger and A. Zeilinger Eds, Ann. N.Y. Acad. Sci. **755**, 73 (1995).

178. E. Schrödinger, *Naturwissenschaften* **23**, 807, 823, 844 (1935). Reprinted in english in J.A. Wheeler and W.H. Zurek, *Quantum theory of measurement*, Princeton University Press (1983).
179. W.H. Zurek, Phys. Rev. D **24**, 1516 (1981).
180. W.H. Zurek, Phys. Rev. D **26**, 1862 (1982).
181. A.O. Caldeira and A.J. Leggett Physica A, **121**, 587 (1983).
182. E. Joos and H.D. Zeh, Z.Phys.B **59**, 223 (1985).
183. W.H. Zurek, Physics Today **44**, 10 p.36 (1991).
184. R. Omnès, *The Interpretation of Quantum Mechanics*, Princeton University Press (1994).
185. D.F. Walls and G.J. Milburn, Phys. Rev. A **31**, 2403.
186. L. Davidovich, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. A **53**, 1295 (1996).
187. M.O. Scully and H. Walther, Phys. Rev. A **39**, 5299 (1989).
188. J.M Raimond, M. Brune and S. Haroche, Phys. Rev. Lett. **79**, 1964 (1997).
189. C.A. Blockey, D.F. Walls, and H. Risken, Europhys. Lett. **17**, 509 (1992).
190. J.I. Cirac, R. Blatt, A.S. Parkins, and P. Zoller, Phys. Rev. Lett. **70**, 762 (1993).
191. J.I. Cirac, R. Blatt, A.S. Parkins, and P. Zoller, Phys. Rev. A **49**, 1202 (1994).
192. J.I. Cirac, R. Blatt, and P. Zoller, Phys. Rev. A **49**, R3174 (1994).
193. Proc.5th Symp.Freq.Standards and Metrology, ed. J.C. Bergquist, (World Scientific, 1996).
194. D.J. Berkeland, J.D. Miller, J.C. Bergquist, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **80**, 2089 (1998).
195. R. Blatt, in *Atomic Physics* **14**, 219, ed. D.J. Wineland, C. Wieman, S.J. Smith, AIP New York (1995).
196. W. Paul, O. Osberghaus, and E. Fischer, Forschungsberichte des Wirtschafts- und Verkehrsministerium Nordrhein-Westfalen **415** (1958).
197. P.K. Ghosh, Ion traps, Clarendon, Oxford (1995).
198. D.J. Wineland, and H. Dehmelt, Bull. Am. Phys. Soc. **20**, 637 (1975).
199. D.J. Wineland, R.E. Drullinger, and F.L. Walls, Phys. Rev. Lett. **40**, 1639 (1978).
200. A. Steane, Appl. Phys. B **64**, 623 (1997), see Table 1 in which a list of candidate ions is given together with relevant experimental parameters.
201. *http://www.bldrdoc.gov/timefreq/ion/index.htm*
202. *http://horology.jpl.nasa.gov/research.html*
203. *http://mste.laser.physik.uni-muenchen.de/lg/worktop.html*
204. *http://p23.lanl.gov/Quantum/quantum.html*

205. *http : //dipmza.physik.uni − mainz.de/ www$_w$erth/calcium/calcium.html*
206. *http : //www − phys.rrz.uni − hamburg.de/home/vms/group$_a$/index.html*
207. *http : //heart − c704.uibk.ac.at/*
208. D.J. Wineland, W.M. Itano, J.C. Bergquist, and R.G. Hulet, Phys. Rev. A **36**, 2220 (1987).
209. J.I. Cirac, A.S. Parkins, R. Blatt, and P. Zoller, Phys. Rev. Lett. **70**, 556 (1993).
210. S. Stenholm, Rev. Mod. Phys. **58**, 699 (1986).
211. C. Monroe, D.M. Meekhof, B.E. King, S.R. Jeffers, W.M. Itano, D.J. Wineland, and P. Gould, Phys. Rev. Lett. **74**, 4011 (1995).
212. H.C. Nägerl, W. Bechter, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Appl. Phys. B **66**, 603 (1998).
213. H.C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. A. **60**, 145 (1999).
214. F. Diedrich, J.C. Bergquist, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **62**, 403 (1989).
215. Ch. Roos, Th. Zeiger, H. Rohde, H.C. Nägerl, J. Eschner, D. Leibfried, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. Lett. **83**, 4713 (1999).
216. B.E. King, C.S. Wood, C.J. Myatt, Q.A. Turchette, D. Leibfried, W.M. Itano, C. Monroe, and D.J. Wineland, Phys. Rev. Lett. **81**, 1525 (1998).
217. H. Dehmelt, Bull. Am. Phys. Soc. **20** 60 (1975).
218. D.J. Wineland, C. Monroe, W.M. Itano, D. Leibfried, B. King, and D.M. Meekhof, Journal of Research of the National Institute of Standards and Technology **103**, 259 (1998).
219. D. Leibfried, D.M. Meekhof, B.E. King, C. Monroe, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett **77**, 4281 (1996).
220. D.M. Meekhof, C. Monroe, B.E. King, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **76**, 1796 (1996).
221. C. Monroe, D.M. Meekhof, B.E. King, and D.J. Wineland, Science **272**, 1131 (1996).
222. J.F. Poyatos, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **77**, 4728 (1996).
223. C. Monroe, D.M. Meekhof, B.E. King, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).
224. L.G. Lutterbach and L. Davidovich, Phys. Rev. Lett. **78**, 2547 (1997).
225. M.B. Plenio and P.L. Knight Phys. Rev. A **53**, 2986 (1996).
226. J.I. Cirac, A.S. Parkins, R. Blatt, and P. Zoller, Adv. At. Molec. Opt. Physics **37**, 238 (1996).
227. D.P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

228. D.J. Wineland, C. Monroe, W.M. Itano, D. Leibfried, B. King, and D.M. Meekhof, Rev. Mod. Phys. (1998).

229. G. Morigi, J. Eschner, J.I. Cirac, and P. Zoller, Phys. Rev. A. **59**, 3797 (1999).

230. E. Peik, J. Abel, T. Becker, J. von Zanthier, and H. Walther, Phys. Rev. A **60**, 439 (1999).

231. I. Waki, S. Kassner, G. Birkl, and H. Walther, Phys. Rev. Lett. **68**, 2007 (1992); G. Birkl, S. Kassner, H. Walther, Nature 357, 310 (1992).

232. D.F.V. James, Appl. Phys. B **66** 181 (1998).

233. C. Monroe, D. Leibfried, B.E. King, D.M. Meekhof, W.M. Itano, and D.J. Wineland, Phys. Rev. **A55**, R2489 (1997).

234. W. Nagourney, J. Sandberg, and H. Dehmelt, Phys. Rev. Lett. **56**, 2797 (1986); Th. Sauter, W. Neuhauser, R. Blatt, and P.E. Toschek, Phys. Rev. Lett. **57**, 1696 (1986); J.C. Bergquist, R. Hulet, W.M. Itano, and D.J. Wineland, Phys. Rev. Lett. **57**, 1699 (1986).

235. P.J. Hore, *Nuclear Magnetic Resonance*, Oxford University Press, Oxford (1995).

236. R.R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions*, Oxford University Press, Oxford (1987).

237. D.G. Cory, A.F. Fahmy, and T.F. Havel, *Proceedings of the Fourth Workshop on Physics and Computation, Nov. 22–24, 1996*, New England Complex Systems Institute, Cambridge, MA (1996).

238. D.G. Cory, A.F. Fahmy, and T.F. Havel, Proc. Natl. Acad. Sci. USA **94,** 1634 (1997).

239. N.A. Gershenfeld and I.L. Chuang, Science **275,** 350 (1997).

240. A. Abragam, *Principles of Nuclear Magnetism*, Clarendon Press, Oxford (1961).

241. C.P. Slichter, *Principles of Magnetic Resonance* 3rd ed. Springer, Berlin, Heidelberg (1990).

242. M. Goldman, *Quantum Description of High-Resolution NMR in Liquids*, Clarendon Press, Oxford (1988).

243. J.A. Jones and M. Mosca, J. Chem. Phys. **109**, 1648 (1998).

244. A. Barenco. C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A, **52**, 3457 (1995).

245. J.A. Jones, R.H. Hansen, and M. Mosca, J. Magn. Reson. **135**, 353 (1998).

246. L.M.K. Vandersypen, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, Phys. Rev. Lett. **83**, 3085 (1999).

247. E. Knill, I. Chuang, and R. Laflamme, Phys. Rev. A, **57**, 3348 (1998).
248. T.F. Havel, S.S. Somaroo, C.-H. Tseng, and D.G. Cory, LANL E-print quant-ph/9812026.
249. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. Lond. A **454**, 339 (1998).
250. I.L. Chuang, L.M.K. Vandersypen, X.L. Zhou, D.W. Leung, and S. Lloyd, Nature, **393**, 143 (1998).
251. I.L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80,** 3408 (1998).
252. J.A. Jones, M. Mosca, and R.H. Hansen, Nature, **393**, 344 (1998).
253. L.K. Grover, Science, **280**, 228 (1998).
254. J.A. Jones and M. Mosca, Phys. Rev. Lett. **83**, 1050 (1999).
255. R. Laflamme, E. Knill, W.H. Zurek, P. Catasti, and S.V.S. Mariappan, Phil. Trans. Roy. Soc. Lond A, **356**, 1941 (1998).
256. R.J. Nelson, D.G. Cory, S. Lloyd, LANL E-print quant-ph/9905028.
257. D.G. Cory, M.D. Price, W. Maas, E. Knill, R. Laflamme, W.H. Zurek, T.F. Havel, and S.S. Somaroo, Phys. Rev. Lett. **81**, 2152 (1998).
258. D. Leung, L. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. Chuang, Phys. Rev. A **60**, 1924 (1999).
259. M.A. Nielsen, E. Knill, and R. Laflamme, Nature, **396**, 52 (1998).
260. N. Linden, H. Barjat, and R. Freeman, Chem. Phys. Lett. **296**, 61 (1998).
261. R. Marx, A. F. Fahmy, J. M. Myers, W. Bermel, and S. J. Glaser, LANL E-print quant-ph/9905087.
262. W.S. Warren, Science, **277**, 1688 (1997).
263. G. Navon, Y.-Q. Song, T. Rõõm, S. Appelt, R.E. Taylor, and A. Pines, Science, **271**, 1848 (1996).
264. L. J. Schulman and U. Vazirani, LANL E-print quant-ph/9804060.
265. R. Freeman, *Spin Choreography*, Spektrum, Oxford, (1997).
266. N. Linden, H. Barjat, R.J. Carbajo, and R. Freeman, Chem. Phys. Lett. **305**, 28 (1999).
267. D.W. Leung, I.L. Chuang, F. Yamaguchi, and Y. Yamamoto, LANL E-print quant-ph/9904100.
268. J.A. Jones and E. Knill, J. Magn. Reson. in press, LANL E-print quant-ph/9905008.
269. N. Linden, Ē. Kupče, and R. Freeman, LANL E-print quant-ph/9907003.
270. P.T. Callaghan, *Principles of Nuclear Magnetic Resonance Microscopy*, Clarendon Press, Oxford (1991).
271. B.E. Kane, Nature **393**, 133 (1998).
272. S.L. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and

R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).

273. R. Schack and C. M. Caves, LANL E-print quant-ph/9903101.
274. T. Pellizzari *et al*, Phys. Rev. Lett. **75** , 3788 (1995).
275. C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995).
276. Q. Turchette *et al.*, Phys. Rev. Lett. **75**, 4710 (1995).
277. K. Mattle *at al.*, Phys. Rev. Lett. **76**, 4656 (1996).
278. J. I. Cirac, P. Zoller, H.J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).
279. C.H. Bennett, Physics Today **24**, (October 1995) and references cited; A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); W. Tittel *et al.*, quant-ph/9707042; W.T. Buttler *et al.*, quant-ph/9801006.
280. C.H. Bennett *et al*, Phys. Rev. Lett. **70**, 1895 (1993); D. Bouwmeester *et al.*, Nature **390**, 575 (1997); D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).
281. L.K. Grover, quant-ph/9704012.
282. A.K. Ekert *et al.*, quant-ph/9803017.
283. C.K. Law and J.H. Eberly, Phys. Rev. Lett. **76**, 1055 (1996).
284. H.J. Carmichael, Phys. Rev. Lett. **70**, 2273 (1993).
285. For a review see P. Zoller and C.W. Gardiner in *Quantum Fluctuations*, Les Houches, ed. E. Giacobino *et al.*, Elsevier, NY, in press.
286. C.W. Gardiner, Phys. Rev. Lett.**70**, 2269 (1993).
287. P.W. Shor, Phys. Rev. A **52**, R2493 (1995); A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996); J.I. Cirac, T. Pellizzari and P. Zoller, Science **273**, 1207 (1996); P. Shor, *Fault–tolerant quantum computation*, quant–ph/9605011; D. DiVincenzo and P.W. Shor, Phys. Rev. Lett. **77**, 3260 (1996).
288. C.H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996); D. Deutsch *et al.*, Phys. Rev. Lett. **77** , 2818 (1996); N. Gisin, Phys. Lett. A **210**, 151 (1996).
289. D.M. Greenberger, M.A. Horne, A. Zeilinger, A. Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe,* edited by M. Kafatos, (Kluwer, Dordrecht, 1989) pp. 73-76.
290. D.M. Greenberger, M.A. Horne,A. Shimony, A. Zeilinger, Bell's theorem without inequalities. Am. J. Phys. **58**, 1131 (1990).
291. D. Bouwmeester, J.-W.. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Observation of three-photon Greenberger-Horne-Zeilinger entanglement. Phys. Rev. Lett. **82**, 1345 (1999).
292. D.M. Greenberger, M.A. Horne, A. Zeilinger, Multiparticle interferometry and the superposition principle. Physics Today, 22, August 1993.
293. N.D. Mermin, Am. J. Phys. **58**, 731 (1990).
294. N.D. Mermin, What's wrong with these elements of reality? Physics To-

day, 9, June 1990.

295. S.J. Freedman and J.S. Clauser, Experimental test of local hidden-variable theories. Phys. Rev. Lett. **28**, 938-941 (1972).

296. A. Aspect, J. Dalibard, and G. Roger, Experimental test of Bell's inequalities using time-varying analysers. Phys. Rev. Lett. **47**, 1804-1807 (1982).

297. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Violation of Bell's inequality under strict Einstein locality conditions. Phys. Rev. Lett. **81**, 5039-5043 (1998).

298. L. Hardy, Nonlocality for two particles without inequalities for almost all entagled states. Phys. Rev. Lett. **71**, 1665-1668 (1993).

299. D. Boschi, S. Branca, F. De Martini, and L. Hardy, Ladder proof of nonlocality without inequalities: Theoretical and experimental results. Phys. Rev. Lett. **79**, 2755 (1997).

300. A. Zeilinger, M.A. Horne, H. Weinfurter, and M. Zukowski, Three particle entanglements from two entangled pairs. Phys. Rev. Lett. **78**, 3031-3034 (1997).

301. S. Haroche, Ann. N. Y. Acad. Sci. **755**, 73 (1995); J.I. Cirac, P. Zoller, Phys. Rev. A **50**, R2799 (1994).

302. S. Lloyd, Phys. Rev. A **57**, R1473 (1998); R. Laflamme, E. Knill, W.H. Zurek, P. Catasti, S.V.S. Mariappan, Phil.Trans. R. Soc. Lond. A **356**, 1941 (1998).

303. S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A **57**, 822 (1998).

304. M. Zukowski, A. Zeilinger, H. Weinfurter, Entangling photons radiated by independent pulsed source. Ann. NY Acad. Sci. **755**, 91-102 (1995).

305. M.A. Horne, Fortschr. Phys. **46**, 6 (1998).

306. G. Krenn, A. Zeilinger, Phys. Rev. A. **54**, 1793 (1996).

307. Z.Y. Ou and L. Mandel, Violation of Bell's inequality and classical probability in a two-photon correlation experiment. Phys. Rev. Lett. **61**, 50-53 (1988).

308. Y.H. Shih and C.O. Alley, New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion. Phys. Rev. Lett. **61**, 2921-2924 (1988).

309. P. Kwiat, P.E. Eberhard, A.M. Steinberger, and R.Y. Chiao, Proposal for a loophole-free Bell inequality experiment. Phys. Rev. A **49**, 3209-3220 (1994).

310. L. De Caro and A. Garuccio, Reliability of Bell-inequality measurements using polarisation correlations in parametric-down-conversion photons. Phys. Rev. A **50**, R2803-R2805 (1994).

311. S. Popescu, L. Hardy, and M. Zukowski, Revisiting Bell's theorem for a class of down-conversion experiments. Phys. Rev. A. **56**, R4353-4357 (1997).
312. M. Zukowski, Violations of local realism in multiphoton interference experiments. quant-ph/9811013.
313. J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Experimental test of quantum nonlocality in three-photn Greenberger–Horne–Zeilinger entanglement, Nature **403**, 515 (2000).
314. N.D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states. Phys. Rev. Lett. **65**, 1838-1841 (1990).
315. S.M. Roy and V. Singh,Tests of signal locality and Einstein-Bell locality for multiparticle systems. Phys. Rev. Lett. **67**, 2761-2764 (1991).
316. M. Zukowski and D. Kaszlikowski, Critical visibility for N-particle Greenberger-Horne-Zeilinger correlations to violate local realism. Phys. Rev. A **56**, R1682-1685 (1997).
317. The original reference is E. Schmidt, *Zur Theorie der linearen und nicht linearen Integralgleichungen*, Math. Annalen **63**, 433 (1907), in the context of quantum theory see H. Everett III, in *The Many-World Interpretation of Quantum Mechanics*, ed. B.S. DeWitt and N. Graham, Princeton University Press, Princeton, 3 (1973), and H. Everett III, Rev. Mod. Phys. **29**, 454 (1957). A graduate level textbook by A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht, (1993), Chapt. 5 includes a brief description of the Schmidt decomposition; A. Ekert and P.L. Knight, Am. J. Phys., **63**, 415 (1995).
318. A. Peres, "Higher order Schmidt Decompositions", lanl-gov e-print server no. 9504006, 1995.
319. J. von Neumann, "Mathematische Grundlagen der Quantenmechanik" (Springer, Berlin, 1932; English Translation, Princeton University Press, Princeton, 1955).
320. M. Horodecki, P. Horodecki, and R. Horodecki, *Mixed-state entanglement and distillation: is there a "bound" entanglement in nature?*, lanl gov e-print quant-ph/9801069.
321. V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
322. V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
323. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
324. W.K. Wootters, *Entanglement of Formation of an Arbitrary State of Two Qubits*, lanl e-print server quant-ph/9709029, (1997); S. Hill and

W.K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

325. T. Rockafeller, *Convex Analysis*, Princeton University Press, New Jersey, (1970).

326. N. Gisin, Phys. Lett. **A 210**, 151 (1996), and references therein; A. Peres, Phys. Rev. A **54**, 2685 (1996); M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **223**, 1 (1996).

327. V. Vedral, M.B. Plenio, K. Jacobs, and P.L. Knight, Phys. Rev. A **56**, 4452 (1997).

328. W.K. Wootters, Phys. Rev. D **23**, 357 (1981).

329. T.M. Cover and J.A. Thomas, *Elements of Information Theory*, Wiley-Interscience,(1991).

330. F. Hiai and D. Petz, Comm. Math. Phys. **143**, 99 (1991).

331. M. Hayashi, *Asymptotic Attainment for Quantum Relative Entropy*, lanl e-print server: quant-ph/9704040 (1997).

332. W.H. Zurek, Physics Today, 36 (October 1991).

333. G.M. Palma, K.-A. Suominen, and A.K. Ekert, Proc. R. Soc. London A. **452**, 567 (1996).

334. D. DiVincenzo, Phys. Rev. A, **50**, 1015 (1995).

335. W. Unruh, Phys. Rev. A, **51**, 992 (1995).

336. D. Loss and D. DiVincenzo, Phys. Rev. A, **57**, 120 (1998).

337. A. Barenco et.al, Phys. Rev. Lett. **74**, 4083 (1995).

338. C. Cohen-Tannoudji, J. Dupont-Roc, and Grynberg, *Atom Photon Interaction*, John Wiley (1992).

339. M. Gross and S. Haroche, Phys. Rep. **93**, 301 (1982).

340. A. Crubellier, S. Liberman, D. Pavolini, and A. Pillet, J. Phys. B, **18**, 3811 (1985).

341. P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

342. D.G. Cory, M.D. Price, T.F. Havel, Physica D **120**, 82 (1998).

343. N.A. Gershenfeld and I.L. Chuang, Science, **275**, 350 (1997).

344. P.L. Knight, M.B. Plenio and V. Vedral, Phil. Trans. Roc. Soc. Lond. A, **355**, 2381 (1997).

345. M.B. Plenio and P.L. Knight, Phys. Rev. A, **53**, 2986 (1996).

346. M.B. Plenio and P.L. Knight, Proc. R. Soc. Lond. A, **453**, 2017 (1997).

347. M.B. Plenio and P.L. Knight, *New Developments on Fundamental Problems in Quantum Physics*, edited by M. Ferrero and A. van der Merwe, Kluwer, Dordrecht, 311 (1997).

348. A. Garg, Phys. Rev. Lett. **77**, 964 (1996).

349. R.J. Hughes, D.F.V. James, E.H. Knill, R. Laflamme, and A.G. Petschek, Phys. Rev. Lett. **77**, 3240 (1996).

350. P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos,* CA IEEE Computer Society Press, New York, 124 (1994).
351. V. Vedral, A. Barenco, and A. Ekert, Phys. Rev. A, **54**, 147 (1996).
352. D. Deutsch, (1993) talk presented at the Rank Prize Funds Mini–Symposium on Quantum Communication and Cryptography, Broadway, England; A. Berthiaume, D. Deutsch and R. Jozsa, in *Proceedings of Workshop on Physics and Computation — PhysComp94*, IEEE Computer Society Press, Dallas, Texas, (1994).
353. A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa and C. Macchiavello, SIAM J. Comput. **26**, 1541 (1997).
354. Ash, *Information Theory*, Dover (1996).
355. A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
356. R. Laflamme, C. Miquel, J.P. Paz and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
357. A. Steane, Error correcting codes in quantum theory, Phys. Rev. Lett. **77**, 793 (1995).
358. A. Steane, Multiple particle interference and quantum error correction, Proc. R. Soc. Lond. A, **452**, 2551 (1995).
359. J. Preskill, Reliable quantum computers, Proc. Roy. Soc. Lond. A, **454**, 469 (1998).
360. D. Gottesman, Class of quantum error-correcting codes saturating the quantum Hamming bound, Phys. Rev. A, **54**, 1862 (1996).
361. A.R. Calderbank, E.M. Rains, N.J.A. Sloane and P.W. Shor, Quantum error correction and orthogonal geometry, Phys. Rev. Lett. **78** 405 (1997).
362. A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Information Theory **44** 1369 (1998).
363. P.W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A, **52**, R2493 (1995).
364. A.R. Calderbank and P.W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A, **54**, 1098 (1996).
365. E. Knill and R. Laflamme, A theory of quantum error correcting codes, Phys. Rev. A, **55**, 900 (1997).
366. E. Knill and R. Laflamme, Concatenated quantum codes, LANL eprint quant-ph/9608012.
367. P.W. Shor, Fault-tolerant quantum computation, in *Proc. 37th Symp. on Foundations of Computer Science*, (Los Alamitos, CA: IEEE Computer Society Press), pp15-65 (1996).

368. A.M. Steane, Space, time, parallelism and noise requirements for reliable quantum computing, Fortschr. Phys. **46**, 443 (1998). (LANL eprint quant-ph/9708021).

369. D. Aharonov and M. Ben-Or, Fault-Tolerant Quantum Computation With Constant Error Rate, LANL eprint quant-ph/9906129.

370. E. Knill, R. Laflamme and W.H. Zurek, Resilient quantum computation: Error Models and Thresholds, Proc. Roy. Soc. Lond A **454**, 365 (1998); Science **279**, 342 (1998). (LANL eprint quant-ph/9702058).

371. A.M. Steane, Active stabilisation, quantum computation and quantum state synthesis, Phys. Rev. Lett. **78**, 2251 (1997).

372. A.M. Steane, Efficient fault-tolerant quantum computing, Nature, vol. **399**, 124-126 (May 1999). (LANL eprint quant-ph/9809054).

373. D. Gottesman, A theory of fault-tolerant quantum computation, Phys. Rev. A **57**, 127 (1998). (LANL eprint quant-ph/9702029).

374. W.H. Itano et al., Phys. Rev. A, **47**, 3554 (1993).

375. W.J. Wineland et al., Phys. Rev. A, **46**, R6797 (1992).

376. D. J. Wineland et al., Phys. Rev. A, **50**, 67 (1994).

377. J.J. Bollinger et al., Phys. Rev. A, **54**, R4649 (1996).

378. C.W. Gardiner, *Quantum Noise*, Springer–Verlag, Berlin (1991).

379. S.F. Huelga, C. Macchiavello, T. Pellizari, A.K. Ekert, M.B. Plenio and J.I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).

380. A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa and C. Macchiavello, SIAM J. Comput. **26**, 1541 (1997).

381. H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

382. N. Gisin, Phys. Lett. A **210**, 151 (1996).

383. M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998); Phys. Rev. Lett. **82**, 1056 (1999).

384. E.M. Rains, Phys. Rev. A **60**, 173 (1999).

385. A. Kent, N. Linden, and S. Massar, Los Alamos preprint quant-ph/9802022.

386. G. Giedke, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 2641 (1999).

387. W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999); ibid. **60**, 729 (1999).

388. B. Huttner, J.D. Gautier, A. Muller, H. Zbinden and N. Gisin, Phys. Rev. A, **54**, 3783 (1996).

389. M. Horodecki P. Horodecki and M. Horodecki. Violating bell inequality by mixed spin 1/2 states: necessary and sufficient condition. Phys. Lett.

A, **200**, 340 (1995).

390. C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
391. M. Murao, M.B. Plenio, S. Popescu, V. Vedral and P.L. Knight, Phys. Rev. A **57**, R4075 (1998).
392. N. Linden S. Popescu, Fortsch. Phys. **46**, 567 (1998).
393. S.J. van Enk, J.I. Cirac, and P. Zoller, Phys. Rev. Lett., **78**, 4293 (1997).
394. S.J. van Enk, J.I. Cirac, and P. Zoller, Science, **279**, 205 (1998).
395. J.I. Cirac, et al, Physica Scripta, Proceedings of the Nobel Symposium 104, Modern Studies of Basic Quantum Concepts and Phenomena, Uppsala, Sweden, June 13-17 (1997).
396. R.J. Glauber, In *Frontiers in Quantum Optics*, (eds. E.R. Pike and S. Sarkar), 534, Adam Hilger, Bristol (1986).
397. S.J. van Enk, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **79**, 5178 (1997).
398. M. Zukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993); see also S. Bose *et al.*, Phys. Rev. A, **57**, 822 (1998); J.-W. Pan *et al.*, Phys. Rev. Lett. **80**, 3891 (1998).
399. E. Knill and R. Laflamme, quant/ph-9608012. See also A. Yu. Kitaev, Russ. Math. Surv. **52**, 1191 (1997); D. Aharonov and M. Ben-Or, quant-ph/9611025; C. Zalka, quant-ph/ 9612028.
400. P. Shor, quant-ph/9605011; A.M. Steane, Phys. Rev. Lett. **78**, 2252 (1997). D. Gottesman, Phys. Rev. A **57**, 127 (1998); For a review see, for example, J. Preskill, in *Introduction to Quantum Computation*, ed. by H.K. Lo, S. Popescu and T.P. Spiller.

訳者あとがき

本書の原書 *The Physics of Quantum Information* は，2000 年に Springer から刊行された．原書の副題は,「量子暗号，量子テレポーテーション，量子計算」となっていて，近年，発展著しい量子情報科学に関する文字通り網羅的内容のテキストとなっている．これだけ内容が充実している単行本は，今日にいたるまで，ほかに例がない．

しかも，歳月を経ても，色あせることのない重要な内容が網羅されていることに改めて驚かされる．そのことは，原書の編者である Dirk Bouwmeester, Artur Ekert と Anton Zeilinger が類い希なる慧眼の持ち主であることを示している．当該分野の代表的研究者である彼らだからこそ，適材適所の第一線の研究者たちに，原書の各章の分担執筆を依頼できたのである．

そして，そのようなすばらしい内容の原書の翻訳を，国内の，やはり第一線で活躍する研究者の方々にお願いして完成したのが本書である．本書の訳出には，思いの外，時間がかかってしまったが，それは日進月歩のこの分野において，多忙を極める第一線の研究者に翻訳を分担していただくことのむずかしさを示している．

既に欧米のベンチャーから量子暗号装置が製品として売り出されている．2007 年 2 月には，カナダのベンチャー企業 D-Wave が 16 量子ビットの量子コンピューティングのデモンストレーションをシリコンバレーで行ったとの報道がなされるに至った．このほかにもさまざまな関連するニュースが報道され，量子情報科学分野がますます注目を集めているこの時期に，本書を世

に送り出せることに大きな意義を感じている．本書が契機となって，さらに多くの方々に，この活発な先端科学技術分野に対する興味をもっていただければ，訳者一同にとって，これほどの喜びはない．

共立出版編集部の石井徹也氏には，訳者多忙のため，遅れを極めた翻訳作業を終始辛抱強く見守っていただき，大変丁寧な編集作業でサポートしていただいた．この場をお借りして，深く感謝申し上げたい．

2007 年 4 月 24 日

西野哲朗

索　　引

タ　行

ナ　行

ハ　行

〈監訳者紹介〉

西野哲朗（にしの てつろう）

略　歴：1984年　早稲田大学理工学研究科数学専攻博士前期課程 修了
　　　　1984年　日本アイ・ビー・エム（株）東京基礎研究所 研究員
　　　　1987年　東京電機大学理工学部情報科学科 助手
　　　　1992年　北陸先端科学技術大学院大学 助教授
　　　　1994年　電気通信大学電子情報学科 助教授
　　　　1999年　電気通信大学情報通信工学科 助教授
　　　　2006年　同教授
現　在：電気通信大学情報通信工学科 教授，理学博士
著訳書：『計算量理論概説』（朝倉書店，共著）
　　　　『コンピュータ基礎理論ハンドブック』（丸善，共訳）
　　　　『形式言語理論入門』（東京電機大学出版局，翻訳）
　　　　『属性文法入門』（共立出版，共著）
　　　　『量子コンピュータ入門』（東京電機大学出版局）
　　　　『中国人郵便配達問題＝コンピュータサイエンス最大の難関』（講談社）
　　　　『形式言語の理論』（丸善，共著）
　　　　『量子コンピューティング』（シュプリンガー・フェアラーク東京，共訳）
　　　　『量子コンピュータと量子暗号』（岩波書店）
　　　　『量子コンピュータの理論』（培風館）他

井元信之（いもと のぶゆき）

略　歴：1977年　東京大学大学院工学系研究科修士課程 修了
　　　　1977年　NTT 物性科学基礎研究所
　　　　1990年　英国エセックス大学 客員研究員
　　　　1999年　総合研究大学院大学 教授
　　　　2004年　大阪大学大学院基礎工学研究科 教授
現　在：大阪大学大学院基礎工学研究科 教授，工学博士
著訳書：『レーザー測定』（丸善，共著）
　　　　『アインシュタインとボーア』（裳華房，共著）他

量子情報の物理
―量子暗号，量子テレポーテーション，量子計算―

（原題 *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*）

2007 年 5 月 25 日　初版 1 刷発行

監訳者　西野哲朗，井元信之　© 2007
原著編者　D. Bouwmeester（バウミースター）
　　　　A. Ekert（エカート）
　　　　A. Zeilinger（ツァイリンガー）
発行者　南 條 光 章
発行所　**共立出版株式会社**
東京都文京区小日向 4-6-19
電話　03-3947-2511（代表）
郵便番号　112-8700
振替口座　00110-2-57035
URL http://www.kyoritsu-pub.co.jp/

印　刷　啓文堂
製　本　関山製本

社団法人
自然科学書協会
会員

検印廃止
NDC007

ISBN 978-4-320-03431-0

Printed in Japan